Docket No.: 56937-108 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Hidenori NANKI, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: January 27, 2004	:	Examiner: Unknown

For: INFORMATION PROCESSING APPARATUS

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-026810, filed February 4, 2003

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:tlb
Facsimile: (202) 756-8087
Date: January 27, 2004

56937-108
NANKI et al.
January 27, 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　２月　４日
出願番号 Application Number:	特願２００３－０２６８１０
[ST. 10/C]:	[ＪＰ２００３－０２６８１０]
出願人 Applicant(s):	松下電器産業株式会社

２００３年１０月２９日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０８９５８７

【書類名】　特許願
【整理番号】　5037740051
【あて先】　特許庁長官　殿
【国際特許分類】　G06B　9/06
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　南木　秀憲
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　吉岡　志郎
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　川口　謙一
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　甲斐　俊也
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　深井　慎一郎
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100086737

【弁理士】

【氏名又は名称】　岡田　和秀

【電話番号】　06-6376-0857

【手数料の表示】

【予納台帳番号】　007401

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9305280

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置

【特許請求の範囲】

【請求項１】　ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

ＣＰＵによる演算処理に用いられ、データの受け渡しを行い、その内部にデータを格納する機能を持つ汎用レジスタと、

前記汎用レジスタに付加され、前記ユーザメモリ空間から前記汎用レジスタのデータ部へのデータ転送が行われた場合はセキュリティ不要状態にセットされ、前記セキュアメモリ空間から前記汎用レジスタのデータ部にデータ転送が行われた場合はセキュリティ必要状態にセットされることが可能であるセキュア情報部と、

前記汎用レジスタのデータを前記ユーザメモリ空間に書き込む際に、前記セキュア情報部の値がセキュリティ必要状態かセキュリティ不要状態かを判別し、前記ユーザメモリ空間へのデータ転送を禁止するか否かの制御を行う機能を持つデータ制御部と、

前記アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、前記セキュア情報部の値を選択する機能を持つアドレス制御部とを備えることを特徴とする情報処理装置。

【請求項２】　前記データ制御部から入力される命令コードを格納する際に、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、ユーザプログラムとセキュアプログラムのどちらが実行されているかを前記データ制御部に知らせる機能を持つ命令フェッチアドレス制御部と、

前記ＣＰＵによる命令フェッチ処理に用いられ、前記データ制御部から入力された命令コードをその内部に格納する機能を持つ命令バッファと、

前記ユーザメモリ空間上に配置されており、主にユーザによってプログラミングされるユーザプログラムと、

前記セキュアメモリ空間上に配置されており、主に開発者によってプログラミ

ングされ、ユーザにはその内容は非公開であるセキュアプログラムとを備え、

前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記命令フェッチアドレス制御部によって、前記ユーザメモリ空間から命令をフェッチしてきたことが判別された場合で、かつ、前記セキュア情報部の値がセキュリティ必要状態である場合、前記ユーザメモリ空間へのデータ転送を禁止することを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記ＣＰＵによる演算処理に用いられ、前記データ制御部とデータの受け渡しを行い、その内部にデータを格納する機能を持つ複数の汎用レジスタと、

前記各汎用レジスタに付加されており、前記アドレス制御部の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態またはセキュリティ無効状態の値をセットすることが可能である複数のセキュア情報部と、

演算命令を実行して前記各汎用レジスタを用いて２つ以上のレジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも１つ以上含む場合は、演算結果を格納する汎用レジスタのセキュア情報部をセキュリティ無効状態とする機能を持つ汎用レジスタファイルとを備え、

前記データ制御部は、前記セキュア情報部がセキュリティ無効状態の汎用レジスタに対する演算命令を行う際に、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は演算を禁止することを特徴とする請求項２に記載の情報処理装置。

【請求項４】　前記ＣＰＵによる演算処理に用いられ、比較演算処理等の結果を比較フラグとして値を保持する機能を持ち、演算命令を実行して、２つ以上の汎用レジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも１つ以上含む場合で、かつ、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は、各フラグの値を変化させない状態レジスタを備えることを特徴とする請求項２に記載の情報処理装置。

【請求項５】　前記ユーザメモリ空間に外部からアクセスを行う際に使用される読み書き可能なＩＯ空間であるユーザＩＯ空間と、

前記セキュアメモリ空間に外部からアクセスを行う際に使用される読み書き可能なＩＯ空間であるセキュアＩＯ空間と、

前記セキュアＩＯ空間に接続して使用され、デバッグ鍵を含むデータを内部に格納する機能を持つＩＣカードと、

前記ＩＣカード内部に格納されており、開発者がユーザシステムで前記セキュアプログラムのデバッグを行う際に、前記セキュアＩＯ空間を介してＣＰＵに読み出されると、前記命令フェッチアドレス制御部と前記アドレス制御部のアドレス判別機能を停止させる機能を持つデバッグ鍵とを備え、

前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記デバッグ鍵がＣＰＵに読み出された場合には、前記ユーザメモリ空間と前記セキュアメモリ空間のどちらから命令をフェッチしてきた場合も前記ユーザメモリ空間へのデータ転送を禁止しない機能を持つことを特徴とする請求項２に記載の情報処理装置。

【請求項６】　ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータをＣＰＵ内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つセキュア情報付き内蔵ＲＡＭ空間と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制

御を行うことを特徴とする情報処理装置。

【請求項７】　ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をＣＰＵ内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つセキュア情報付き命令デコーダと、

前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つセキュア情報付き内蔵ＲＡＭ空間と、

割り込み等の処理が発生した際に、前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つセキュア情報付き割り込み退避情報部と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うことを特徴とする情報処理装置。

【請求項８】　ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をＣＰＵ内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令

かを判別する機能を持つセキュア情報付き命令デコーダと、

前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つセキュア情報付き内蔵ＲＡＭ空間と、

割り込み等の処理が発生した際に、前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つセキュア情報付き割り込み退避情報部と、

前記セキュア情報付き内蔵ＲＡＭ空間の一部をスタック領域に定義するスタックポインタと、

前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域の書き換え制御を行う退避情報書き換え制御部とを備え、

前記退避情報書き換え制御部は、前記セキュア情報付き命令デコーダの命令がユーザメモリ空間の命令でかつ前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域を書き換えようとした命令の場合には、その書き換えを禁止することを特徴とする情報処理装置。

【請求項９】　ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

セキュア情報を保持する機能を持つセキュア情報付きＤＭＡと、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータを前記セキュア情報付きＤＭＡ内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きＤＭＡから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付きＤＭＡに受け渡す機能を持つセキュア情報付き内蔵ＲＡＭ空間と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付きＤＭＡにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うことを特徴とする情報処理装置。

【請求項１０】　ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をＣＰＵ内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つセキュア情報付き命令デコーダと、

前記セキュア情報付き命令デコーダでデコードされた命令により実行される演算に前記セキュア情報付き命令デコーダのセキュア情報を反映する機能を持つセキュア情報付き演算部と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報及び前記セキュア情報付き演算部にセットされた前記セキュア情報により前記外部空間へのデータ転送を禁止するか否かの制御を行うことを特徴とする情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置に関するものである。

【０００２】

【従来の技術】

従来、例えばＳＤカードのセキュリティを守るのに、暗号解読をハードが行い、ＳＤカード内の暗号データと暗号鍵とを用いて暗号を解読し、暗号化されていないデータに復号化していた。これが将来的には、複数の暗号化に対応するためにＰＤＡ（personal digital assistants:携帯情報端末）等でのコンテンツサー

ビスでは暗号解読をソフトで行うようになる可能性がある。従来は、ＯＳ（operatingsystem）の特権モードと通常モードでユーザがアクセスできる領域を切り分けることによって、また、メモリマネジメントユニット等のハードウエアのメモリ保護機能によって、暗号解読ソフトの外部漏洩を防いでいた。

【０００３】

【特許文献１】

特開平６－２６６６２４号公報（第３－６頁、図１－図３）

【０００４】

【発明が解決しようとする課題】

しかしながら、オープンソースなＯＳである例えばＬｉｎｕｘを使ったＰＤＡでは、ソフトウェア開発環境が広くユーザに開示されることになる。これにより、アプリケーションの開発が行いやすくなる反面、Ｌｉｎｕｘ等の開示された開発環境で、ユーザがＯＳの持つ特権モードを利用して、ユーザモードではアクセスできないセキュリティのかけられた空間のデータを読み出し、ユーザＲＡＭ空間や外部空間への転送を行うことでＯＳのデバッグ作業を行っていたような従来技術を利用して、セキュリティ空間に置かれた暗号鍵やデータや命令を盗むといった悪用が簡単にできてしまう可能性があるという課題が出てくる。

【０００５】

また、わが国では平成１２年１２月よりＢＳデジタル放送が開始され、放送のデジタル化が進むとともに、放送されたデジタルコンテンツの著作権が侵害される問題も発生している。そのため、放送コンテンツ提供者の中には、コンテンツを提供するに当って厳格な著作権保護を求める者も現れており、放送メディアのデジタル化とデジタルコンテンツの円滑な流通を促進させるためには、放送コンテンツの権利保護のための何らかの措置が必要になってくる。

【０００６】

本発明は、かかる点に鑑み、暗号解読アルゴリズムが明らかであってもオープンな開発環境に与えられる特権モードを利用するだけでは、セキュアメモリ空間の暗号鍵やデータや命令を読むことについて、これをできないようにすることで、将来的に行われる可能性の高い悪用を回避する情報処理装置を提供することを

目的とする。

【０００７】

【課題を解決するための手段】

上記の課題を解決するために、本発明は次のような手段を講じる。

【０００８】

（１）第１の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～汎用レジスタ、セキュア情報部、データ制御部およびアドレス制御部を備えている。前記汎用レジスタは、ＣＰＵによる演算処理に用いられ、データの受け渡しを行い、その内部にデータを格納する機能を持つ。前記セキュア情報部は、前記汎用レジスタに付加され、前記ユーザメモリ空間から前記汎用レジスタのデータ部へのデータ転送が行われた場合はセキュリティ不要状態にセットされ、前記セキュアメモリ空間から前記汎用レジスタのデータ部にデータ転送が行われた場合はセキュリティ必要状態にセットされることが可能である。前記データ制御部は、前記汎用レジスタのデータを前記ユーザメモリ空間に書き込む際に、前記セキュア情報部の値がセキュリティ必要状態かセキュリティ不要状態かを判別し、前記ユーザメモリ空間へのデータ転送を禁止するか否かの制御を行う機能を持つ。前記アドレス制御部は、前記アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、前記セキュア情報部の値を選択する機能を持つ。

【０００９】

上記構成による作用は次のとおりである。汎用レジスタにセキュア情報部である付加ビットを設けるだけで、ＣＰＵの命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュリティ空間からユーザ空間へのデータ複写を禁止することができる。すなわち、セキュアプログラムの解読（ハッキング）を防ぐことができる。

【００１０】

（２）第２の解決手段として、本発明による情報処理装置は、上記の第１の解

決手段において、さらに、それぞれ次のような機能を有する構成要素～命令フェッチアドレス制御部、命令バッファ、ユーザプログラムおよびセキュアプログラムを備えている。前記命令フェッチアドレス制御部は、前記データ制御部から入力される命令コードを格納する際に、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、ユーザプログラムとセキュアプログラムのどちらが実行されているかを前記データ制御部に知らせる機能を持つ。前記命令バッファは、前記ＣＰＵによる命令フェッチ処理に用いられ、前記データ制御部から入力された命令コードをその内部に格納する機能を持つ。前記ユーザプログラムは、前記ユーザメモリ空間上に配置されており、主にユーザによってプログラミングされるものである。前記セキュアプログラムは、前記セキュアメモリ空間上に配置されており、主に開発者によってプログラミングされ、ユーザにはその内容は非公開である。さらに、前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記命令フェッチアドレス制御部によって、前記ユーザメモリ空間から命令をフェッチしてきたことが判別された場合で、かつ、前記セキュア情報部の値がセキュリティ必要状態である場合、前記ユーザメモリ空間へのデータ転送を禁止するように構成されている。

【００１１】

上記構成による作用は次のとおりである。開発者がセキュアメモリ空間でのセキュアプログラムの開発を行う場合には、ユーザメモリ空間とセキュアメモリ空間の領域間の自由なＬＯＡＤ／ＳＴＯＲＥの特権を与えることができ、ユーザがユーザメモリ空間でのユーザプログラムの開発を行う場合には、セキュアメモリ空間からユーザメモリ空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムとユーザプログラムとで、セキュアメモリ空間のデータを自由に扱える権限の切り分けが可能である。

【００１２】

（３）第３の解決手段として、本発明による情報処理装置は、上記第２の解決手段において、さらに、それぞれ次のような機能を有する構成要素～複数の汎用レジスタ、複数のセキュア情報部および汎用レジスタファイルを備えている。前

記複数の汎用レジスタは、前記ＣＰＵによる演算処理に用いられ、前記データ制御部とデータの受け渡しを行い、その内部にデータを格納する機能を持つ。前記複数のセキュア情報部はそれぞれ、前記各汎用レジスタに付加されており、前記アドレス制御部の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態またはセキュリティ無効状態の値をセットすることが可能である。前記汎用レジスタファイルは、演算命令を実行して前記各汎用レジスタを用いて２つ以上のレジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも１つ以上含む場合は、演算結果を格納する汎用レジスタのセキュア情報部をセキュリティ無効状態とする機能を持つ。さらに、前記データ制御部は、前記セキュア情報部がセキュリティ無効状態の汎用レジスタに対する演算命令を行う際に、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は演算を禁止するように構成されている。

【００１３】

上記構成による作用は次のとおりである。セキュアメモリ空間のデータを格納したレジスタの内容に対して、ユーザプログラムの演算処理による操作（例えば、セキュアメモリ空間からレジスタに読み出したデータと、オール“１”のデータとのＡＮＤ演算を行った結果を、別のレジスタに格納するようなダミー演算などを行う操作）をできなくすることで、セキュアメモリ空間のメモリ内容の推測を防ぎ、セキュアプログラムの解読（ハッキング）を防ぐことができる。

【００１４】

（４）第４の解決手段として、本発明による情報処理装置は、上記第２の解決手段において、さらに、次のような機能を有する状態レジスタを備えるものである。その状態レジスタは、前記ＣＰＵによる演算処理に用いられ、比較演算処理等の結果を比較フラグとして値を保持する機能を持ち、演算命令を実行して、２つ以上の汎用レジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも１つ以上含む場合で、かつ、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は、各フラグの値を変化させないもの

である。

【００１５】

上記構成による作用は次のとおりである。ユーザプログラムが、比較演算処理等の結果を比較フラグとして値を保持する状態レジスタを用いて２値以上のレジスタ比較を行ったとしても、セキュアメモリ空間のデータを格納したレジスタ内容の比較による推測を防ぎ、セキュアプログラムの解読を防ぐことができる。

【００１６】

（５）第５の解決手段として、本発明による情報処理装置は、上記第２の解決手段において、さらに、それぞれ次のような機能を有する構成要素～ユーザＩＯ空間、セキュアＩＯ空間、ＩＣカードおよびデバッグ鍵を備えている。前記ユーザＩＯ空間は、前記ユーザメモリ空間に外部からアクセスを行う際に使用される読み書き可能なＩＯ空間である。前記セキュアＩＯ空間は、前記セキュアメモリ空間に外部からアクセスを行う際に使用される読み書き可能なＩＯ空間である。前記ＩＣカードは、前記セキュアＩＯ空間に接続して使用され、デバッグ鍵を含むデータを内部に格納する機能を持つ。前記デバッグ鍵は、前記ＩＣカード内部に格納されており、開発者がユーザシステムで前記セキュアプログラムのデバッグを行う際に、前記セキュアＩＯ空間を介してＣＰＵに読み出されると、前記命令フェッチアドレス制御部と前記アドレス制御部のアドレス判別機能を停止させる機能を持つ。さらに、前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記デバッグ鍵がＣＰＵに読み出された場合には、前記ユーザメモリ空間と前記セキュアメモリ空間のどちらから命令をフェッチしてきた場合も前記ユーザメモリ空間へのデータ転送を禁止しない機能を持つものに構成されている。

【００１７】

上記構成による作用は次のとおりである。開発者がユーザシステムでセキュアプログラムのデバッグを行う際には、汎用レジスタのセキュア情報付加ビットの機能は停止され、ユーザメモリ空間とセキュアメモリ空間の領域間での自由なデータ転送が可能となり、セキュアプログラムをモニタリングできるようになる。すなわち、ユーザの環境においても、開発者はデバッグ鍵が格納されたＩＣカー

ドによりセキュアプログラムを容易にデバッグでき、従来の特権モードと同義の権利を得られる。

【００１８】

（６）第６の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き内蔵ＲＡＭ空間およびデータ出力制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータをＣＰＵ内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き内蔵ＲＡＭ空間は、前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【００１９】

上記構成による作用は次のとおりである。汎用レジスタにセキュア情報のための付加ビットを設けるだけで、ＣＰＵの命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュアメモリ空間から外部空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムの解読(ハッキング)を防ぐことができる。

【００２０】

さらに、セキュア情報付き内蔵ＲＡＭ空間を経由するデータのセキュリティ管理を可能とし、データ自身にセキュア情報を付加するため、内蔵ＲＡＭ空間にセキュアメモリ空間のデータとユーザメモリ空間のデータの混在を可能とする。そ

して、ユーザメモリ空間の命令により、セキュア情報付き内蔵ＲＡＭ空間上のセキュアデータの書き換えを許可し、通常使用に影響がない状態でセキュア情報付き内蔵ＲＡＭ空間のセキュリティ管理を可能とすることができる。

【００２１】

（７）第７の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き命令デコーダ、セキュア情報付き内蔵ＲＡＭ空間、セキュア情報付き割り込み退避情報部およびデータ出力制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をＣＰＵ内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き命令デコーダは、実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つ。前記セキュア情報付き内蔵ＲＡＭ空間は、前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つ。前記セキュア情報付き割り込み退避情報部は、割り込み等の処理が発生した際に、前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【００２２】

上記構成による作用は次のとおりである。割り込み等によるセキュア情報付き内蔵ＲＡＭ空間への退避データにセキュア情報を付加することにより、内蔵ＲＡＭ空間に自動的に退避されたデータの読み出しにおけるセキュリティ管理を可能

にする。したがって、セキュアメモリ空間の重要なタスクのハッキングを防御することができる。

【００２３】

（８）第８の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き命令デコーダ、セキュア情報付き内蔵ＲＡＭ空間、セキュア情報付き割り込み退避情報部、スタックポインタおよび退避情報書き換え制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をＣＰＵ内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き命令デコーダは、実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つ。前記セキュア情報付き内蔵ＲＡＭ空間は、前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つ。前記セキュア情報付き割り込み退避情報部は、割り込み等の処理が発生した際に、前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つ。前記スタックポインタは、前記セキュア情報付き内蔵ＲＡＭ空間の一部をスタック領域に定義する。前記退避情報書き換え制御部は、前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域の書き換え制御を行う。さらに、前記退避情報書き換え制御部は、前記セキュア情報付き命令デコーダの命令がユーザメモリ空間の命令でかつ前記セキュア情報付き内蔵ＲＡＭ空間のスタック領域を書き換えようとした命令の場合には、その書き換えを禁止するものである。

【００２４】

上記構成による作用は次のとおりである。セキュアメモリ空間の命令実行中にユーザ割り込み等によって、セキュア情報付き内蔵ＲＡＭ空間に退避されたセキ

ュアメモリ空間への戻り先番地等を、ユーザメモリ空間の命令から書き換えることを禁止することにより、セキュアメモリ空間への正常な復帰を保証するとともに、ユーザメモリ空間の命令に許可されていないセキュアメモリ空間へのアクセスを制限し、なおかつ、前記セキュア情報付き内蔵ＲＡＭ空間の通常領域とスタック領域を物理的に分割せずに、スタックポインタの指し示す空間による書き換え制御の切り替えでスタック領域のセキュリティ管理ができる。

【００２５】

（９）第９の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報付きＤＭＡ、セキュア情報生成部、セキュア情報付き内蔵ＲＡＭ空間およびデータ出力制御部を備えている。前記セキュア情報付きＤＭＡは、セキュア情報を保持する機能を持つ。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータを前記セキュア情報付きＤＭＡ内部に受け渡す。前記セキュア情報付き内蔵ＲＡＭ空間は、前記セキュア情報付きＤＭＡから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付きＤＭＡに受け渡す機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付きＤＭＡにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【００２６】

上記構成による作用は次のとおりである。ＣＰＵが介在しないＤＭＡ転送データに対してもセキュア情報を追従させ、ＤＭＡを経由するデータのセキュリティ管理を可能とし、セキュアメモリ空間のデータ及び命令をセキュア情報付きＤＭＡによりセキュア情報付き内蔵ＲＡＭ空間に展開して使用する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能とし、セキュア情報付き内蔵ＲＡＭ空間のデータ及び命令をセキュア情報付きＤＭＡにより外部

空間に転送する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能にする。

【００２７】

（１０）第１０の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き命令デコーダ、セキュア情報付き演算部およびデータ出力制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をＣＰＵ内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き命令デコーダは、実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つ。前記セキュア情報付き演算部は、前記セキュア情報付き命令デコーダでデコードされた命令により実行される演算に前記セキュア情報付き命令デコーダのセキュア情報を反映する機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報及び前記セキュア情報付き演算部にセットされた前記セキュア情報により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【００２８】

上記構成による作用は次のとおりである。セキュアメモリ空間の命令であり、かつ、演算を行う命令を実行する場合、被演算対象となる全データがユーザメモリ空間のデータであっても、またはセキュア情報部にセキュアデータであることが明示されていなくても、セキュアメモリ空間の命令に付加されるセキュア情報をセキュア情報付き演算部のセキュア情報に反映することにより、演算結果が外部空間に流出することを防ぎ、演算結果からセキュアメモリ空間の命令内容を類推することを防御することができる。

【００２９】

【発明の実施の形態】

以下、本発明にかかわる情報処理装置の実施の形態を図面に基づいて説明する。

【００３０】

（実施の形態１）

図１は本発明の実施の形態１における情報処理装置の構成を示す概念図であり、図中、１００は情報処理装置、１０１はＣＰＵ、１０２は汎用レジスタファイル、１０３は汎用レジスタ、１０４はセキュア情報部、１０５はデータ制御部、１０６はアドレス制御部、１０７はデータ／アドレスバス、１１０はユーザメモリ空間（ＲＡＭ）、１２０はセキュアメモリ空間（ＲＯＭ）である。このうち、情報処理装置１００は装置の全体ブロックであり、外部にユーザメモリ空間１１０とセキュアメモリ空間１２０が接続されている。

【００３１】

ＣＰＵ１０１は、汎用レジスタファイル１０２を持ち、ユーザメモリ空間１１０とセキュアメモリ空間１２０にアクセスし、汎用レジスタ１０３へデータの読み書きを行う。汎用レジスタファイル１０２は、汎用レジスタ１０３とそれに対応したセキュア情報部１０４を持つ。汎用レジスタ１０３は、ＣＰＵ１０１による演算処理に用いられ、データ制御部１０５とデータの受け渡しを行い、その内部にデータを格納する機能を持つ。セキュア情報部１０４は、汎用レジスタ１０３に付加されており、アドレス制御部１０６の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態の値をセットすることが可能である。

【００３２】

データ制御部１０５は、データ／アドレスバス１０７から入力されたデータを汎用レジスタファイル１０２に書き込み、また汎用レジスタファイル１０２から受け取ったデータをデータ／アドレスバス１０７に出力してユーザメモリ空間１１０に書き込む際に、セキュア情報部１０４の値を判別して、書き込みを禁止するか否かの制御を行う機能を持つ。

【００３３】

アドレス制御部１０６は、データ／アドレスバス１０７から入力されたアドレス情報がユーザメモリ空間１１０とセキュアメモリ空間１２０のどちらを示しているかを判別し、汎用レジスタファイル１０２内のセキュア情報部１０４の値を選択する機能を持つ。

【００３４】

データ／アドレスバス１０７は、データ制御部１０５、アドレス制御部１０６、外部メモリデータバス１３０、外部メモリアドレスバス１４０を接続し、それぞれの間でのデータまたはアドレスの受け渡しを行う機能を持つ。

【００３５】

ユーザメモリ空間１１０は、読み書き可能なメモリであり、外部メモリアドレスバス１４０から入力されたアドレス情報によって、外部メモリデータバス１３０とデータの入出力を行う機能を持つ。

【００３６】

セキュアメモリ空間１２０は、読み出しのみが可能なメモリであり、外部メモリアドレスバス１４０から入力されたアドレス情報によって、外部メモリデータバス１３０にデータを出力する機能を持つ。

【００３７】

外部メモリデータバス１３０は、情報処理装置１００と、ユーザメモリ空間１１０またはセキュアメモリ空間１２０間のデータの受け渡しを行う機能を持つ。

【００３８】

外部メモリアドレスバス１４０は、情報処理装置１００から受け取ったアドレス情報をユーザメモリ空間１１０またはセキュアメモリ空間１２０に渡す機能を持つ。

【００３９】

次に、上記のように構成された実施の形態１の情報処理装置の動作について説明する。

【００４０】

図２は実施の形態１の動作を示すフローチャートであり、図中、６０１はＬＯＡＤ命令発行処理、６０２はＬＯＡＤアドレス判別処理、６０３はセキュリティ

必要処理、６０４はセキュリティ不要処理、６０５は汎用レジスタＳＴＯＲＥ処理、６０６はＳＴＯＲＥ命令発行処理、６０７はセキュリティ状態判別処理、６０８はユーザメモリ空間ＳＴＯＲＥ処理、６０９はユーザメモリ空間ＳＴＯＲＥ禁止処理である。

【００４１】

ＬＯＡＤ命令発行処理６０１は、ＣＰＵ１０１が外部メモリに対してＬＯＡＤ命令を発行する処理であり、この処理を終えるとＬＯＡＤアドレス判別処理６０２に移行する。

【００４２】

ＬＯＡＤアドレス判別処理６０２は、アドレス制御部１０６がデータ／アドレスバス１０７から入力されたアドレス情報がセキュアメモリ空間１２０であるかそうでないかを判別し、セキュアメモリ空間１２０であるとき、セキュリティ必要処理６０３に移行し、そうでないとき（ユーザメモリ空間１１０であるとき）、セキュリティ不要処理６０４に移行する。

【００４３】

セキュリティ必要処理６０３は、アドレス制御部１０６がセキュア情報部１０４の値をセキュリティ必要状態にセットする処理であり、この処理を終えると汎用レジスタＳＴＯＲＥ処理６０５に移行する。

【００４４】

セキュリティ不要処理６０４は、アドレス制御部１０６が、セキュア情報部１０４の値をセキュリティ不要状態にセットする処理であり、この処理を終えると汎用レジスタＳＴＯＲＥ処理６０５に移行する。

【００４５】

汎用レジスタＳＴＯＲＥ処理６０５は、ＣＰＵ１０１が、外部メモリから外部メモリデータバス１３０、データ／アドレスバス１０７、データ制御部１０５を介して受け取ったデータを汎用レジスタ１０３にストアする処理であり、この処理を終えるとＳＴＯＲＥ命令発行処理６０６に移行する。

【００４６】

ＳＴＯＲＥ命令発行処理６０６は、ＣＰＵ１０１が外部メモリに対してＳＴＯ

ＲＥ命令を発行する処理であり、この処理を終えるとセキュリティ状態判別処理６０７に移行する。

【００４７】

セキュリティ状態判別処理６０７は、データ制御部１０５がセキュア情報部１０４の値がセキュリティ不要状態であるかそうでないかを判別し、セキュリティ不要状態であるとき、ユーザメモリ空間ＳＴＯＲＥ処理６０８に移行し、そうでないとき（セキュリティ必要状態であるとき）、ユーザメモリ空間ＳＴＯＲＥ禁止処理６０９に移行する。

【００４８】

ユーザメモリ空間ＳＴＯＲＥ処理６０８は、ＣＰＵ１０１が、汎用レジスタ１０３から受け取ったデータを、データ制御部１０５、データ／アドレスバス１０７、外部メモリデータバス１３０を介してユーザメモリ空間１１０にストアする処理であり、この処理を終えると動作完了である。

【００４９】

ユーザメモリ空間ＳＴＯＲＥ禁止処理６０９は、ＣＰＵ１０１が、汎用レジスタ１０３から受け取ったデータを、データ制御部１０５、データ／アドレスバス１０７、外部メモリデータバス１３０を介してユーザメモリ空間１１０にストアすることを禁止する処理であり、この処理を終えると動作完了である。

【００５０】

以上の構成により、レジスタにセキュア情報部である付加ビットを設けるだけで、ＣＰＵの命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュリティ空間からユーザ空間へのデータ複写を禁止することができる。すなわち、セキュアプログラムの解読（ハッキング）を防ぐことができるという格別の効果を奏する。

【００５１】

（実施の形態２）

上記の実施の形態１には次のような課題がある。すなわち、セキュアプログラムがセキュアメモリ空間で実行されている場合、例えば有料音楽配信サービスな

どで、配信されたＭＰ３コンテンツをデコードし、デコードされたＷＡＶＥデータをユーザメモリ空間へ転送する、またはプログラム実行時に使用する関数の呼び出しを行い、必要なデータをユーザメモリ空間に一時的に退避しなければならない場合、セキュアメモリ空間からユーザメモリ空間へのデータ転送が発生する。このような場合にデータ転送を禁止すると、セキュアプログラムの動作内容が制限されるという課題が発生する。従って、ユーザプログラムによる転送であるのか、セキュアプログラムによる転送であるかの切り分けが可能となる新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態２である。以下、実施の形態２の情報処理装置の構成について説明する。

【００５２】

図３は本発明の実施の形態２における情報処理装置の構成を示す概念図であり、図中、実施の形態１において説明した図１と同様のブロックについては、同一の番号を付し、その説明を省略する。

【００５３】

１０８は命令フェッチアドレス制御部、１０９は命令バッファ、１１０ｐはユーザプログラム、１２０ｐはセキュアプログラムである。

【００５４】

このうち、命令フェッチアドレス制御部１０８は、命令バッファ１０９を持ち、データ制御部１０５から入力される命令コードを命令バッファ１０９に格納する際に、データ／アドレスバス１０７から入力されるアドレス情報がユーザメモリ空間１１０とセキュアメモリ空間１２０のどちらを示しているかを判別し、ユーザプログラム１１０ｐとセキュアプログラム１２０ｐのどちらが実行されているかをデータ制御部１０５に知らせる機能を持つ。

【００５５】

命令バッファ１０９は、ＣＰＵ１０１による命令フェッチ処理に用いられ、データ制御部１０５から入力された命令コードをその内部に格納する機能を持つ。

【００５６】

ユーザプログラム１１０ｐは、ユーザメモリ空間１１０上に配置されており、主にユーザによってプログラミングされる。

【００５７】

セキュアプログラム１２０ｐは、セキュアメモリ空間１２０上に配置されており、主に開発者によってプログラミングされ、ユーザにはその内容は非公開である。

【００５８】

次に、上記のように構成された実施の形態２の情報処理装置の動作について説明する。

【００５９】

図４は実施の形態２の動作を示すフローチャートであり、図中、実施の形態１において説明した図２と同様のフローについては、同一の番号を付し、その説明を省略する。

【００６０】

７０１はＬＯＡＤアドレス判別処理であり、命令フェッチアドレス制御部１０８が、データ／アドレスバス１０７から入力されたアドレス情報がセキュアメモリ空間１２０であるかそうでないかを判別し、セキュアメモリ空間１２０であるとき、ユーザメモリ空間ＳＴＯＲＥ処理６０８に移行し、セキュアメモリ空間１２０でないとき、ユーザメモリ空間ＳＴＯＲＥ禁止処理６０９に移行する。

【００６１】

以上の構成により、開発者がセキュアメモリ空間でのセキュアプログラムの開発を行う場合には、ユーザメモリ空間とセキュアメモリ空間の領域間の自由なＬＯＡＤ／ＳＴＯＲＥの特権を与えることができ、ユーザがユーザメモリ空間でのユーザプログラムの開発を行う場合には、セキュアメモリ空間からユーザメモリ空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムとユーザプログラムとで、セキュアメモリ空間のデータを自由に扱える権限の切り分けが可能であるという格別の効果を奏する。

【００６２】

（実施の形態３）

上記の実施の形態１には、また次のような課題がある。すなわち、ユーザのプログラムによる汎用レジスタを介したセキュアメモリ空間からユーザメモリ空間

へのデータ転送を禁止することは可能であるが、例えば汎用レジスタ同士の演算を行った場合、その演算結果を新たなレジスタに格納してユーザメモリ空間にストアする行為は禁止されていない。例えば、セキュアメモリ空間からレジスタに読み出したデータと、オール“１”のデータとのＡＮＤ演算を行った結果を、別のレジスタに格納するようなダミー演算を行うことで、セキュアメモリ空間のデータを容易に推測できるといった課題が発生する。従って、ユーザプログラムの演算に使用できるデータに制限をかけることが可能となる新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態３である。以下、実施の形態３の情報処理装置の構成について説明する。

【００６３】

図５は本発明の実施の形態３における情報処理装置の構成を示す概念図であり、図中、実施の形態１，２において説明した図１、図３と同様のブロックについては、同一の番号を付し、その説明を省略する。

【００６４】

３００は第１の汎用レジスタ、３０１は第２の汎用レジスタ、３０２は第３の汎用レジスタ、３０３は第１のセキュア情報部、３０４は第２のセキュア情報部、３０５は第３のセキュア情報部である。

【００６５】

このうち、第１の汎用レジスタ３００、第２の汎用レジスタ３０１、第３の汎用レジスタ３０２は、ＣＰＵ１０１による演算処理に用いられ、データ制御部１０５とデータの受け渡しを行い、その内部にデータを格納する機能を持つ。

【００６６】

第１のセキュア情報部３０３、第２のセキュア情報部３０４、第３のセキュア情報部３０５は、それぞれ第１の汎用レジスタ３００、第２の汎用レジスタ３０１、第３の汎用レジスタ３０２に付加されており、アドレス制御部１０６の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態またはセキュリティ無効状態の値をセットすることが可能である。

【００６７】

次に、上記のように構成された実施の形態３の情報処理装置の動作について説

明する。

【００６８】

図６は実施の形態３の動作を示すフローチャートであり、図中、実施の形態１，２において説明した図２、図４と同様のフローについては、同一の番号を付し、その説明を省略する。

【００６９】

８０１は汎用レジスタ（１～２）ＳＴＯＲＥ処理、８０２はＣＰＵ演算命令（１～２）発行処理、８０３はセキュリティ状態（１）判別処理、８０４はセキュリティ状態（２）判別処理、８０５はセキュリティ（３）無効処理、８０６はセキュリティ（３）不要処理、８０７は汎用レジスタ（３）演算結果格納処理、８０８はＣＰＵ演算命令（３）発行処理、８０９はセキュリティ状態（３）判別処理、８１０は演算禁止処理、８１１はＣＰＵクリア命令（３）発行処理、８１２はセキュリティ（３）不要処理である。

【００７０】

汎用レジスタ（１～２）ＳＴＯＲＥ処理８０１は、ＣＰＵ１０１が外部メモリから外部メモリデータバス１３０、データ／アドレスバス１０７、データ制御部１０５を介して受け取ったデータを第１の汎用レジスタ３００、第２の汎用レジスタ３０１にストアする処理であり、この処理を終えるとＣＰＵ演算命令（１～２）発行処理８０２に移行する。

【００７１】

ＣＰＵ演算命令（１～２）発行処理８０２は、ＣＰＵ１０１が第１の汎用レジスタ３００、第２の汎用レジスタ３０１を用いて何らかの演算処理（ＡＤＤ，ＳＵＢなど）を行う処理であり、この処理を終えるとセキュリティ状態（１）判別処理８０３に移行する。

【００７２】

セキュリティ状態（１）判別処理８０３は、データ制御部１０５が第１のセキュア情報部３０３の値がセキュリティ必要状態であるかそうでないかを判別し、セキュリティ必要状態であるとき、セキュリティ（３）無効処理８０５に移行し、そうでないとき（セキュリティ不要状態であるとき）、セキュリティ状態（２

）判別処理８０４に移行する。

【００７３】

セキュリティ状態（２）判別処理８０４は、データ制御部１０５が第２のセキュア情報部３０４の値がセキュリティ必要状態であるかそうでないかを判別し、セキュリティ必要状態であるとき、セキュリティ（３）無効処理８０５に移行し、そうでないとき（セキュリティ不要状態であるとき）、セキュリティ（３）不要処理８０６に移行する。

【００７４】

セキュリティ（３）不要処理８０６は、アドレス制御部１０６が第３のセキュア情報部３０５の値をセキュリティ不要状態にセットする処理であり、この処理を終えると汎用レジスタ（３）演算結果格納処理８０７に移行する。

【００７５】

汎用レジスタ（３）演算結果格納処理８０７は、第１の汎用レジスタ３００、第２の汎用レジスタ３０１の演算処理結果を第３の汎用レジスタ３０２に格納する処理であり、この処理を終えるとＣＰＵ演算命令（３）発行処理８０８に移行する。

【００７６】

ＣＰＵ演算命令（３）発行処理８０８は、ＣＰＵ１０１が第３の汎用レジスタ３０２を用いて何らかの演算処理（ＳＴＯＲＥ，ＪＵＭＰなど）を行う処理であり、この処理を終えるとセキュリティ状態（３）判別処理８０９に移行する。

【００７７】

セキュリティ状態（３）判別処理８０９は、データ制御部１０５が第３のセキュア情報部３０５の値がセキュリティ無効状態であるかそうでないかを判別し、セキュリティ無効状態であるとき、演算禁止処理８１０に移行し、そうでないとき（セキュリティ不要状態またはセキュリティ必要状態であるとき）、ＣＰＵクリア命令（３）発行処理８１１に移行する。

【００７８】

ＣＰＵクリア命令（３）発行処理８１１は、ＣＰＵ１０１が第３の汎用レジスタ３０２に対してクリア演算処理（ＣＬＲ）を行う処理であり、この処理を終え

るとセキュリティ（３）不要処理８１２に移行する。

【００７９】

セキュリティ（３）不要処理８１２は、アドレス制御部１０６が第３のセキュア情報部３０５の値をセキュリティ不要状態にセットする処理であり、この処理を終えると動作完了である。

【００８０】

以上の構成により、セキュアメモリ空間のデータを格納したレジスタの内容に対して、ユーザプログラムの演算処理（ＡＤＤ（＋），ＳＵＢ（－），ＭＵＬ（×），ＤＩＶ（÷）などの四則演算）による操作をできなくすることで、セキュアメモリ空間のメモリ内容の推測を防ぐことができる。例えば、セキュアメモリ空間からレジスタに読み出したデータと、オール“１”のデータとのＡＮＤ演算を行った結果を、別のレジスタに格納するようなダミー演算などを行うことで、セキュアメモリ空間のデータ推測（8’ b11010011 & 8’ b11111111 = 8’ b11010011）、すなわち、セキュアプログラムの解読（ハッキング）を防ぐという格別の効果を奏する。

【００８１】

（実施の形態４）

上記の実施の形態１には、また次のような課題がある。すなわち、ユーザのプログラムによる２値以上のレジスタ比較を行った場合、演算結果を知らずとも、比較演算処理の結果を保持する状態レジスタを参照すれば、容易にセキュアメモリ空間のデータを推測できるといった課題が発生する。世の中に存在する多くのＣＰＵでは状態レジスタを持つものがほとんどであり、従って、ユーザプログラムの状態レジスタを用いた演算に制限をかける新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態４である。以下、実施の形態４の情報処理装置の構成について説明する。

【００８２】

図７は本発明の実施の形態４における情報処理装置の構成を示す概念図であり、図中、実施の形態１～３において説明した図１、図３、図５と同様のブロックについては、同一の番号を付し、その説明を省略する。

【００８３】

４００は状態レジスタであり、ＣＰＵ１０１による演算処理に用いられ、比較演算処理等の結果を比較フラグとして値を保持する機能を持つ。

【００８４】

次に、上記のように構成された実施の形態４の情報処理装置の動作について説明する。

【００８５】

図８は実施の形態４の動作を示すフローチャートであり、図中、実施の形態１～３において説明した図２、図４、図６と同様のフローについては、同一の番号を付し、その説明を省略する。

【００８６】

９０１は汎用レジスタ（１～２）比較演算処理、９０２は状態レジスタ比較フラグ変更禁止処理、９０３は状態レジスタ比較フラグ変更処理である。

【００８７】

汎用レジスタ（１～２）比較演算処理９０１は、ＣＰＵ１０１が第１の汎用レジスタ３００、第２の汎用レジスタ３０１を用いて比較演算処理（ＣＭＰなど）を行う処理であり、この処理を終えるとセキュリティ状態（１）判別処理８０３に移行する。

【００８８】

状態レジスタ比較フラグ変更禁止処理９０２は、汎用レジスタ（１～２）比較演算処理９０１の比較演算結果を受けて、状態レジスタ４００の比較フラグの値を変更することを禁止する処理であり、この処理を終えると動作完了である。

【００８９】

状態レジスタ比較フラグ変更処理９０３は、汎用レジスタ（１～２）比較演算処理９０１の比較演算結果を受けて、状態レジスタ４００の比較フラグの値を変更する処理であり、この処理を終えると動作完了である。

【００９０】

以上の構成により、ユーザプログラムが、比較演算処理等の結果を比較フラグとして値を保持する状態レジスタを用いて２値以上のレジスタ比較を行ったとし

ても、セキュアメモリ空間のデータを格納したレジスタ内容の比較による推測を防ぐことができる。すなわち、セキュアプログラムの解読を防ぐという格別の効果を奏する。

【００９１】

（実施の形態５）

以上実施の形態１～４において、開発者がユーザシステムでセキュアプログラムのデバッグを行う際には、ユーザメモリ空間においてセキュアプログラムをモニタリングしなければならないので、セキュアメモリ空間からユーザメモリ空間へのデータ転送が禁止されているとデバッグできないといった課題が発生する。従って、レジスタを介したデータ転送を禁止する機能を解除する新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態５である。以下、実施の形態５の情報処理装置の構成について説明する。

【００９２】

図９は本発明の実施の形態５における情報処理装置の構成を示す概念図であり、図中、実施の形態１～４において説明した図１、図３、図５、図７と同様のブロックについては、同一の番号を付し、その説明を省略する。

【００９３】

５００は端末ＰＣ、５０１はユーザＩＯ空間（ＲＡＭ）、５０２はセキュアＩＯ空間（ＲＡＭ）、５０３はＩＣカード、Ｓ５０３はデバッグ鍵である。

【００９４】

このうち、端末ＰＣ５００は、開発者によってセキュアプログラム１２０ｐのデバッグが行われる際に使用され、ユーザＩＯ空間５０１に接続され、デバッグプログラムをユーザメモリ空間１１０に置いてデバッグを行う機能を持つ。

【００９５】

ユーザＩＯ空間５０１は、ユーザメモリ空間１１０に外部からアクセスを行う際に使用される読み書き可能なＩＯ空間である。

【００９６】

セキュアＩＯ空間５０２は、セキュアメモリ空間１２０に外部からアクセスを行う際に使用される読み書き可能なＩＯ空間である。

【００９７】

ＩＣカード５０３は、セキュアＩＯ空間５０２に接続して使用され、デバッグ鍵Ｓ５０３等のデータを内部に格納する機能を持つ。

【００９８】

デバッグ鍵Ｓ５０３は、ＩＣカード５０３の内部に格納されており、開発者がユーザシステムでセキュアプログラム１２０ｐのデバッグを行う際に、セキュアＩＯ空間５０２を介してＣＰＵ１０１に読み出されると、命令フェッチアドレス制御部１０８とアドレス制御部１０６のアドレス判別機能を停止させる機能を持つ。

【００９９】

次に、上記のように構成された実施の形態５の情報処理装置の動作について説明する。

【０１００】

図１０は実施の形態５の動作を示すフローチャートであり、図中、実施の形態１～４において説明した図２、図４、図６、図８と同様のフローについては、同一の番号を付し、その説明を省略する。

【０１０１】

１００１はデバッグ鍵入力処理、１００２はデバッグ鍵ＬＯＡＤ処理、１００３は命令フェッチアドレス制御部停止処理、１００４はアドレス制御部停止処理である。

【０１０２】

デバッグ鍵入力処理１００１は、ＩＣカード５０３からセキュアＩＯ空間５０２へデバッグ鍵Ｓ５０３を入力する処理であり、この処理を終えるとデバッグ鍵ＬＯＡＤ処理１００２に移行する。

【０１０３】

デバッグ鍵ＬＯＡＤ処理１００２は、ＣＰＵ１０１が、セキュアＩＯ空間５０２から外部メモリデータバス１３０、データ／アドレスバス１０７、データ制御部１０５を介してデバッグ鍵Ｓ５０３を読み出す処理であり、この処理を終えると命令フェッチアドレス制御部停止処理１００３に移行する。

【０１０４】

命令フェッチアドレス制御部停止処理１００３は、命令フェッチアドレス制御部１０８が持つアドレス判別機能を停止する処理であり、この処理を終えるとアドレス制御部停止処理１００４に移行する。

【０１０５】

アドレス制御部停止処理１００４は、アドレス制御部１０６が持つアドレス判別機能を停止する処理であり、この処理を終えるとＬＯＡＤ命令発行処理６０１に移行する。

【０１０６】

以上の構成により、開発者がユーザシステムでセキュアプログラムのデバッグを行う際には、汎用レジスタのセキュア情報付加ビットの機能は停止され、ユーザメモリ空間とセキュアメモリ空間の領域間での自由なデータ転送が可能となり、セキュアプログラムをモニタリングできるようになる。すなわち、ユーザの環境においても、開発者はデバッグ鍵が格納されたＩＣカードにより、セキュアプログラムを容易にデバッグでき、従来の特権モードと同義の権利を得られる、という格別の効果を奏する。

【０１０７】

（実施の形態６）

図１１は本発明の実施の形態６における情報処理装置の構成を示す概念図である。本実施の形態の情報処理装置は、セキュアメモリ空間２０１と、ユーザメモリ空間２０２と、データバス２０３と、アドレスバス２０４と、セキュア情報生成部２０５と、セキュア情報付き内蔵ＲＡＭ空間２０６と、ＣＰＵ２０８と、セキュア情報付き汎用レジスタ２０９と、データ出力制御部２１１と、外部空間２１２とによって構成されている。

【０１０８】

さらに、図１２（ａ），（ｂ）に示すように、セキュア情報付き内蔵ＲＡＭ空間２０６は内部にセキュア情報部２０７を備え、セキュア情報付き汎用レジスタ２０９は内部にセキュア情報部２１０を備えている。

【０１０９】

ＣＰＵ２０８は、セキュアメモリ空間２０１またはユーザメモリ空間２０２のデータを読み出す際にアドレスバス２０４を通じてアドレスを指定する。

【０１１０】

セキュアメモリ空間２０１またはユーザメモリ空間２０２は、アドレスバス２０４で指定されたアドレス情報に従いデータを出力する。

【０１１１】

セキュア情報生成部２０５は、指定したアドレス情報に合致したデータを受け取り、指定したアドレス情報がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらを示しているかを判別し、ユーザメモリ空間２０２のデータである場合にはセキュア情報として“０”を、セキュアメモリ空間２０１のデータである場合にはセキュア情報として“１”を付加したデータをセキュア情報付き汎用レジスタ２０９に受け渡す。セキュア情報はセキュア情報付き汎用レジスタ２０９内のセキュア情報部２１０に格納される。

【０１１２】

セキュア情報付き汎用レジスタ２０９のデータをセキュア情報付き内蔵ＲＡＭ空間２０６と外部空間２１２に転送する場合の動作を、図１３（ａ），（ｂ）を用いて説明する。

【０１１３】

２０６ａはセキュア情報付き内蔵ＲＡＭ空間２０６の第１の状態であり、２０６ｂはＲＡＭ空間２０６の第２の状態であり、２０７ａはセキュア情報部２０７の第１の状態であり、２０７ｂはセキュア情報部２０７の第２の状態であり、２０９ａは汎用レジスタ２０９の第１の状態であり、２０９ｂは汎用レジスタ２０９の第２の状態であり、２１０ａはセキュア情報部２１０の第１の状態であり、２１０ｂはセキュア情報部２１０の第２の状態である。

【０１１４】

ＣＰＵ２０８が汎用レジスタ２０９の第１の状態２０９ａのデータをセキュア情報付き内蔵ＲＡＭ空間２０６の第１の状態２０６ａに書き込むと同時に、セキュア情報部２１０の第１の状態２１０ａの値はセキュア情報部２０７の第１の状態２０７ａに書き込まれ、セキュア情報付き内蔵ＲＡＭ空間２０６の第２の状態

２０６ｂとセキュア情報部２０７の第２の状態２０７ｂとなり、セキュア情報は保持される。

【０１１５】

ＣＰＵ２０８がセキュア情報付き内蔵ＲＡＭ空間２０６の第２の状態２０６ｂのデータを読み出すと、汎用レジスタ２０９の第２の状態２０９ｂにデータが受け渡されると同時に、セキュア情報部２０７の第２の状態２０７ｂはセキュア情報部２１０の第２の状態２１０ｂに受け渡され、セキュア情報付き内蔵ＲＡＭ空間２０６を経由するデータのセキュア情報は保持される。

【０１１６】

ＣＰＵ２０８が外部空間２１２にセキュア情報付き汎用レジスタ２０９のデータを出力する際に、データ出力制御部２１１は、セキュア情報付き汎用レジスタ２０９内のセキュア情報部２１０の値が“１”である場合には外部空間２１２へのデータ出力を禁止する。

【０１１７】

以上の構成により、レジスタに付加ビットを設けるだけで、ＣＰＵの命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュアメモリ空間から外部空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムの解読(ハッキング)を防ぐことができる。

【０１１８】

さらに内蔵ＲＡＭ空間に対してもセキュア情報を追従させ、内蔵ＲＡＭ空間を経由するデータのセキュリティ管理を可能とし、データ自身にセキュア情報を付加するために、内蔵ＲＡＭ空間にセキュアメモリ空間のデータとユーザメモリ空間のデータの混在を可能とし、ユーザメモリ空間の命令により、セキュア情報付き内蔵ＲＡＭ空間上のセキュアデータの書き換えを許可し、通常使用に影響がない状態でセキュア情報付き内蔵ＲＡＭ空間のセキュリティ管理を可能とすることができるという格別の効果を奏する。

【０１１９】

（実施の形態７）

図１４は本発明の実施の形態７における情報処理装置の構成を示す概念図であり、図中、実施の形態６において説明した図１１と同様のブロックについては、同一の番号を付し、その説明を省略する。

【０１２０】

図１４において、２１３は割り込み制御部、２１４はセキュア情報付き割り込み退避情報部、２１６はセキュア情報付き命令デコーダ２１６である。

【０１２１】

図１５（ａ），（ｂ）に示すように、セキュア情報付き割り込み退避情報部２１４は内部にセキュア情報部２１５を備え、セキュア情報付き命令デコーダ２１６は内部にセキュア情報部２１７を備える。

【０１２２】

ＣＰＵ２０８は、セキュアメモリ空間２０１またはユーザメモリ空間２０２のデータリード及び命令フェッチを行う際に、アドレスバス２０４を通じてアドレスを指定する。

【０１２３】

セキュアメモリ空間２０１またはユーザメモリ空間２０２は、アドレスバス２０４で指定されたアドレス情報に従いデータ及び命令を出力する。

【０１２４】

セキュア情報生成部２０５は、指定したアドレス情報に合致したデータ及び命令を受け取り、指定したアドレス情報がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらを示しているかを判別し、ユーザメモリ空間２０２のデータである場合にはセキュア情報として“０”を、セキュアメモリ空間２０１のデータである場合にはセキュア情報として“１”を付加したデータをセキュア情報付き汎用レジスタ２０９に受け渡し、セキュア情報はセキュア情報付き汎用レジスタ２０９内のセキュア情報部２１０（図１２参照）に格納される。

【０１２５】

ユーザメモリ空間２０２の命令である場合にはセキュア情報として“０”を、セキュアメモリ空間２０１の命令である場合にはセキュア情報として“１”を付加した命令をセキュア情報付き命令デコーダ２１６に受け渡し、セキュア情報は

セキュア情報部２１７に格納される。

【０１２６】

セキュア情報付き汎用レジスタ２０９のデータを、セキュア情報付き内蔵ＲＡＭ空間２０６に転送する場合の動作は、実施の形態６において説明した内容と同様であるため、その説明を省略する。

【０１２７】

割り込み制御部２１３により割り込み等の処理が発生した際に、セキュア情報付き内蔵ＲＡＭ空間２０６の一部に自動的に退避するデータに対しセキュリティ管理を行うために、現在実行中の命令がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらの命令かによって、退避するデータにセキュア情報を付加する。

【０１２８】

現在実行中の命令は、セキュア情報付き命令デコーダ２１６内のセキュア情報部２１７の値で判別可能であり、ユーザメモリ空間２０２の命令である場合にはセキュア情報は“０”であり、セキュアメモリ空間２０１の命令である場合にはセキュア情報は“１”である。

【０１２９】

割り込み発生時に自動的に退避される情報がセキュア情報であるかどうかを明示するため、セキュア情報付き割り込み退避情報部２１４内のセキュア情報部２１５にセキュア情報付き命令デコーダ２１６内のセキュア情報部２１７の値を伝搬させる。

【０１３０】

さらに、セキュア情報付き割り込み退避情報部２１４のデータをセキュア情報付き内蔵ＲＡＭ空間２０６の一部に退避すると同時に、セキュア情報付き割り込み退避情報部２１４内のセキュア情報部２１５の値をセキュア情報付き内蔵ＲＡＭ空間２０６内のセキュア情報部２０７（図１２参照）に伝搬させる。これにより、退避するデータのセキュア情報は保持される。

【０１３１】

セキュア情報付き内蔵ＲＡＭ空間２０６のデータをセキュア情報付き汎用レジ

スタ２０９に転送する場合の動作は、実施の形態６において説明した内容と同様であるため、その説明を省略する。

【０１３２】

ＣＰＵ２０８が外部空間２１２にセキュア情報付き汎用レジスタ２０９のデータを出力する際に、データ出力制御部２１１は、セキュア情報付き汎用レジスタ２０９内のセキュア情報部２１０の値が“１”である場合には外部空間２１２へのデータ出力を禁止する。

【０１３３】

以上の構成により、割り込み等によるスタック退避情報にもセキュア情報を付加追従させ、セキュア情報付き内蔵ＲＡＭ空間の一部であるスタック領域に自動的に退避されたデータの読み出しにおけるセキュリティ管理を可能とし、例えば、セキュアメモリ空間の命令実行中の実行ＰＣ（プログラムカウンタ）等が外部空間に読み出されることから起こり得る、セキュアメモリ空間の重要なタスクのハッキングを防御することができるという格別の効果を奏する。

【０１３４】

（実施の形態８）

図１６は本発明の実施の形態８における情報処理装置の構成を示す概念図であり、図中、実施の形態６，７において説明した図１１、図１４と同様のブロックについては、同一の番号を付し、その説明を省略する。

【０１３５】

図１６において、２１８はスタックポインタ、２１９は退避情報書き換え制御部である。

【０１３６】

ＣＰＵ２０８は、セキュアメモリ空間２０１またはユーザメモリ空間２０２のデータリード及び命令フェッチを行う際に、アドレスバス２０４を通じてアドレスを指定する。

【０１３７】

セキュアメモリ空間２０１またはユーザメモリ空間２０２は、アドレスバス２０４で指定されたアドレス情報に従いデータ及び命令を出力する。

【０１３８】

セキュア情報生成部２０５は、指定したアドレス情報に合致したデータ及び命令を受け取り、指定したアドレス情報がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらを示しているかを判別し、ユーザメモリ空間２０２のデータである場合にはセキュア情報として“０”を、セキュアメモリ空間２０１のデータである場合にはセキュア情報として“１”を付加したデータをセキュア情報付き汎用レジスタ２０９に受け渡し、セキュア情報はセキュア情報付き汎用レジスタ２０９内のセキュア情報部２１０（図１２参照）に格納される。また、セキュア情報生成部２０５は、ユーザメモリ空間２０２の命令である場合にはセキュア情報として“０”を、セキュアメモリ空間２０１の命令である場合にはセキュア情報として“１”を付加した命令をセキュア情報付き命令デコーダ２１６に受け渡し、セキュア情報はセキュア情報付き命令デコーダ２１６内のセキュア情報部２１７（図１５参照）に格納される。

【０１３９】

割り込み制御部２１３により割り込み等の処理が発生した際に、セキュア情報付き内蔵ＲＡＭ空間２０６のスタックポインタ２１８の指し示すスタック領域に自動的に退避するデータに対しセキュリティ管理を行うために、現在実行中の命令がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらの命令かによって、退避するデータにセキュア情報を付加する場合の動作は、実施の形態７において説明した内容と同様であるため、その説明を省略する。

【０１４０】

また、セキュア情報付き内蔵ＲＡＭ空間２０６の通常領域及びスタック領域のデータをセキュア情報付き汎用レジスタ２０９に転送する場合の動作は、実施の形態６において説明した内容と同様であるため、その説明を省略する。

【０１４１】

以上の構成により、割り込み等によるスタック退避情報にもセキュア情報を付加追従させ、セキュア情報付き内蔵ＲＡＭ空間の一部であるスタック領域に自動的に退避されたデータの読み出しにおけるセキュリティ管理を可能とする。

【０１４２】

また、セキュア情報付き汎用レジスタ２０９のデータを、セキュア情報付き内蔵ＲＡＭ空間２０６の通常領域に転送（ライト）する場合の動作は、実施の形態６において説明した内容と同様であるため、その説明を省略する。

【０１４３】

また、セキュア情報付き汎用レジスタ２０９のデータを、セキュア情報付き内蔵ＲＡＭ空間２０６のスタック領域に転送（ライト）する場合、退避情報書き換え制御部２１９は、現在実行中の命令がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらかをセキュア情報付き命令デコーダ２１６内のセキュア情報部２１７（図１５参照）の値により判別し、さらに転送する空間のアドレスとスタックポインタ２１８を比較し、ユーザメモリ空間２０２の命令であり、かつスタック領域への転送であった場合には、データの転送を禁止する。

【０１４４】

さらに、セキュア情報付き内蔵ＲＡＭ空間２０６の一部であるスタック領域へのデータの退避及び復帰における動作を、図１７（ａ），（ｂ）を用いて説明する。

【０１４５】

２０６ｃはセキュア情報付き内蔵ＲＡＭ空間２０６の第１の状態であり、２０６ｄはＲＡＭ空間２０６の第２の状態であり、２０７ｃはセキュア情報部２０７の第１の状態であり、２１８ｃはスタックポインタ２１８の第１の状態であり、２１８ｄはスタックポインタ２１８の第２の状態であり、７０１ｃはスタック領域の第１の状態であり、７０１ｄはスタック領域の第２の状態であり、７０２ｃは通常領域の第１の状態であり、７０２ｄは通常領域の第２の状態であり、７０３ｃはスタック退避情報である。

【０１４６】

セキュア情報付き内蔵ＲＡＭ空間２０６の第２の状態２０６ｄを初期状態とする。セキュアメモリ空間２０１の命令実行中に割り込みが発生し、ユーザメモリ空間２０２の処理へ移行する場合、セキュア情報付き割り込み退避情報部２１４のデータがセキュア情報付き内蔵ＲＡＭ空間２０６の第２の状態２０６ｄに退避され、その結果、ＲＡＭ空間２０６の第１の状態２０６ｃ中のスタック退避情報

７０３ｃになる。

【０１４７】

この状態では、スタック退避情報にセキュア情報が付加されているため、スタック退避されたデータの読み出しにおけるセキュリティ管理を可能とし、また、スタック領域の第１の状態７０１ｃは退避情報書き換え制御部２１９によりユーザメモリ空間２０２の命令では書き換えを禁止しているため、スタック退避されたデータの書き込みにおけるセキュリティ管理を可能とする。

【０１４８】

割り込みからの復帰によりスタック退避情報７０３ｃが復帰すると、スタックポインタの第１の状態２１８ｃはスタックポインタの第２の状態２１８ｄとなり、不必要となったスタック退避情報７０３ｃの領域を通常領域の第１の状態７０２ｃに開放され、通常領域の第２の状態７０２ｄとなる。

【０１４９】

以上の構成により、セキュアメモリ空間の命令実行中にユーザ割り込み等によって、セキュア情報付き内蔵ＲＡＭ空間に退避されたセキュアメモリ空間への戻り先番地等を、ユーザメモリ空間の命令から書き換えることを禁止することにより、セキュアメモリ空間への正常な復帰を保証するとともに、ユーザメモリ空間の命令に許可されていないセキュアメモリ空間へのアクセスを制限し、なおかつ、前記セキュア情報付き内蔵ＲＡＭ空間の通常領域とスタック領域を物理的に分割せずに、スタックポインタの指し示す空間による書き換え制御の切り替えでスタック領域のセキュリティ管理ができるという格別の効果を奏する。

【０１５０】

（実施の形態９）

図１８は本発明の実施の形態９における情報処理装置の構成を示す概念図であり、図中、実施の形態６において説明した図１１と同様のブロックについては、同一の番号を付し、その説明を省略する。

【０１５１】

図１８において、２２０はセキュア情報付きＤＭＡである。図１９に示すように、セキュア情報付きＤＭＡ２２０はその内部にセキュア情報部２２１を備えて

いる。

【０１５２】

セキュア情報付きＤＭＡ２２０はセキュアメモリ空間２０１またはユーザメモリ空間２０２からのデータ転送を行う際に、アドレスバス２０４を通じてアドレスを指定する。

【０１５３】

セキュアメモリ空間２０１またはユーザメモリ空間２０２は、アドレスバス２０４で指定されたアドレス情報に従いデータを出力する。

【０１５４】

セキュア情報生成部２０５は、指定したアドレス情報に合致したデータを受け取り、指定したアドレス情報がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらを示しているかを判別し、ユーザメモリ空間２０２のデータである場合にはセキュア情報として“０”を、セキュアメモリ空間２０１のデータである場合にはセキュア情報として“１”を付加したデータをセキュア情報付きＤＭＡ２２０に受け渡す。セキュア情報はセキュア情報付きＤＭＡ２２０内のセキュア情報部２２１に格納される。

【０１５５】

セキュア情報付きＤＭＡ２２０のデータを、セキュア情報付き内蔵ＲＡＭ空間２０６と外部空間２１２に転送する場合の動作は、実施の形態６において説明した内容と同様であるため、その説明を省略する。

【０１５６】

また、セキュア情報付きＤＭＡ２２０は、セキュア情報付き内蔵ＲＡＭ空間２０６からのデータ転送を行う際に、アドレスバス２０４を通じてアドレスを指定する。

【０１５７】

セキュア情報付き内蔵ＲＡＭ空間２０６は、アドレスバス２０４で指定されたアドレス情報に従いセキュア情報部２０７（図１２参照）のセキュア情報を付加したデータを出力する。

【０１５８】

セキュア情報付きＤＭＡ２２０は、指定したアドレス情報に合致したデータを受け取ると同時に、セキュア情報部２０７のセキュア情報をセキュア情報部２２１に反映させることにより、セキュア情報付きＤＭＡ２２０を経由するデータのセキュア情報は保持される。

【０１５９】

以上の構成により、ＣＰＵが介在しないＤＭＡ転送データに対してもセキュア情報を追従させ、ＤＭＡを経由するデータのセキュリティ管理を可能とし、セキュアメモリ空間のデータ及び命令をセキュア情報付きＤＭＡによりセキュア情報付き内蔵ＲＡＭ空間に展開して使用する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能とし、セキュア情報付き内蔵ＲＡＭ空間のデータ及び命令をセキュア情報付きＤＭＡにより外部空間に転送する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能とするという格別の効果を奏する。

【０１６０】

（実施の形態１０）

図２０は本発明の実施の形態１０における情報処理装置の構成を示す概念図であり、図中、実施の形態６において説明した図１１と同様のブロックについては、同一の番号を付し、その説明を省略する。

【０１６１】

図２０において、２１６はセキュア情報付き命令デコーダ、２２２はセキュア情報付き演算部である。図２１に示すように、セキュア情報付き演算部２２２は内部にセキュア情報部２２３を備えている。

【０１６２】

ＣＰＵ２０８は、セキュアメモリ空間２０１またはユーザメモリ空間２０２のデータリード及び命令フェッチを行う際に、アドレスバス２０４を通じてアドレスを指定する。

【０１６３】

セキュアメモリ空間２０１またはユーザメモリ空間２０２は、アドレスバス２０４で指定されたアドレス情報に従いデータ及び命令を出力する。

【０１６４】

セキュア情報生成部２０５は、指定したアドレス情報に合致したデータ及び命令を受け取り、指定したアドレス情報がユーザメモリ空間２０２とセキュアメモリ空間２０１のどちらを示しているかを判別し、ユーザメモリ空間２０２のデータである場合にはセキュア情報として“０”を、セキュアメモリ空間２０１のデータである場合にはセキュア情報として“１”を付加したデータをセキュア情報付き汎用レジスタ２０９に受け渡し、セキュア情報はセキュア情報付き汎用レジスタ２０９内のセキュア情報部２１０（図１２参照）に格納される。また、セキュア情報生成部２０５は、ユーザメモリ空間２０２の命令である場合にはセキュア情報として“０”を、セキュアメモリ空間２０１の命令である場合にはセキュア情報として“１”を付加した命令をセキュア情報付き命令デコーダ２１６に受け渡し、セキュア情報はセキュア情報付き命令デコーダ２１６内のセキュア情報部２１７（図１５参照）に格納される。

【０１６５】

セキュアメモリ空間２０１の演算命令がセキュア情報付き命令デコーダ２１６によりデコードされた結果を受け、セキュア情報付き汎用レジスタ２０９のデータがセキュア情報付き演算部２２２に受け渡され、セキュア情報付き演算部２２２は演算を開始する。

【０１６６】

このとき、被演算対象となる１つ以上のセキュア情報付き汎用レジスタ２０９のデータに付加されるセキュア情報部２１０のセキュア情報が、少なくとも１つ以上“１”である場合、セキュア情報付き演算部２２２内のセキュア情報部２２３にはセキュア情報部２１０のセキュア情報“１”が伝搬し、セキュア情報付き演算部２２２が出力する演算結果のセキュア情報は保持される。

【０１６７】

また、被演算対象となる１つ以上のセキュア情報付き汎用レジスタ２０９のデータに付加されるセキュア情報部２１０のセキュア情報が、全て“０”である場合、セキュア情報付き演算部２２２内のセキュア情報部２２３にはセキュア情報付き命令デコーダ２１６内のセキュア情報部２１７のセキュア情報“１”が伝搬

し、セキュア情報付き演算部２２２が出力する演算結果のセキュア情報は保持される。

【０１６８】

また、ユーザメモリ空間２０２の演算命令がセキュア情報付き命令デコーダ２１６によりデコードされた結果を受け、セキュア情報付き汎用レジスタ２０９のデータがセキュア情報付き演算部２２２に受け渡され、セキュア情報付き演算部２２２は演算を開始する。

【０１６９】

このとき、被演算対象となる１つ以上のセキュア情報付き汎用レジスタ２０９のデータに付加されるセキュア情報部２１０のセキュア情報が、少なくとも１つ以上“１”である場合、セキュア情報付き演算部２２２内のセキュア情報部２２３にはセキュア情報部２１０のセキュア情報“１”が伝搬し、セキュア情報付き演算部２２２が出力する演算結果のセキュア情報は保持される。

【０１７０】

また、被演算対象となる１つ以上のセキュア情報付き汎用レジスタ２０９のデータに付加されるセキュア情報部２１０のセキュア情報が、全て“０”である場合、セキュア情報付き演算部２２２内のセキュア情報部２２３にはセキュア情報付き命令デコーダ２１６内のセキュア情報部２１７のセキュア情報“０”が伝搬し、セキュア情報付き演算部２２２が出力する演算結果はセキュアでないという情報が付加される。

【０１７１】

セキュア情報付き演算部２２２のデータを外部空間２１２に転送する場合の動作は、実施の形態６において説明した内容と同様であるため、その説明を省略する。

【０１７２】

以上の構成により、セキュアメモリ空間の命令であり、かつ、演算を行う命令を実行する場合、被演算対象となる全データがユーザメモリ空間のデータであっても、またはセキュア情報部にセキュアデータであることが明示されていなくても、セキュアメモリ空間の命令に付加されるセキュア情報をセキュア情報付き演

算部のセキュア情報に反映することにより、演算結果が外部空間に流出することを防ぎ、例えば、演算結果からセキュアメモリ空間の命令内容を類推することを防御することができるという格別の効果を奏する。

【０１７３】

【発明の効果】

以上のように本発明によれば、ユーザメモリ空間から汎用レジスタにデータを転送した場合はセキュア情報部の値をセキュリティ不要状態とし、セキュアメモリ空間から汎用レジスタにデータを転送した場合はセキュア情報部の値をセキュリティ必要状態とし、セキュア情報部の値がセキュリティ必要状態である汎用レジスタからユーザメモリ空間へのデータ転送が禁止されるようにする制御を行うことによって、セキュアメモリ空間上の暗号鍵等のセキュアプログラム、セキュアデータが読まれることを防ぐことができる。

【０１７４】

同様に、特権モードと通常モードの切り替え制御を行わずして、セキュアメモリ空間から外部空間へのデータ転送を禁止することができる。さらに、セキュア情報付き内蔵ＲＡＭ空間に対してもセキュア情報を追従させ、内蔵ＲＡＭ空間を経由するデータのセキュリティ管理を可能とする。さらに、セキュアメモリ空間の割り込み退避データの読み出しによるハッキングを防御できる。さらに、ユーザメモリ空間の命令に許可されていないセキュアメモリ空間へのアクセスを制限できる。さらに、ＣＰＵが介在しないＤＭＡ転送データに対してもセキュア情報を追従させ、ＤＭＡを経由するデータのセキュリティ管理を可能とする。さらに、演算結果にもセキュア情報を追従させることにより外部空間への漏洩を防ぎ、セキュアメモリ空間の命令内容を類推することを防御することができる。

【０１７５】

すなわち、セキュア情報部を設けることで、従来のＯＳが行っていた特権モード、通常モードのモード切り替え制御を全て付加ビットにより代行し、かつ僅かなハード変更で事足りる、という利点がある。特に、ＰＤＡやデジタルテレビ等、コンテンツサービスにかかわる商品開発では有利な展開が期待される。

【図面の簡単な説明】

【図１】　本発明の実施の形態１における情報処理装置の構成を示す概念図

【図２】　本発明の実施の形態１における情報処理装置の動作を示すフローチャート

【図３】　本発明の実施の形態２における情報処理装置の構成を示す概念図

【図４】　本発明の実施の形態２における情報処理装置の動作を示すフローチャート

【図５】　本発明の実施の形態３における情報処理装置の構成を示す概念図

【図６】　本発明の実施の形態３における情報処理装置の動作を示すフローチャート

【図７】　本発明の実施の形態４における情報処理装置の構成を示す概念図

【図８】　本発明の実施の形態４における情報処理装置の動作を示すフローチャート

【図９】　本発明の実施の形態５における情報処理装置の構成を示す概念図

【図１０】　本発明の実施の形態５における情報処理装置の動作を示すフローチャート

【図１１】　本発明の実施の形態６における情報処理装置の構成を示す概念図

【図１２】　本発明の実施の形態６～１０におけるセキュア情報付き内蔵ＲＡＭ空間、セキュア情報付き汎用レジスタの概念図

【図１３】　本発明の実施の形態６～９におけるセキュア情報付き内蔵ＲＡＭ空間のアクセス状態図

【図１４】　本発明の実施の形態７における情報処理装置の構成を示す概念図

【図１５】　本発明の実施の形態７，８，１０におけるセキュア情報付き命令デコーダ、セキュア情報付き割り込み退避情報部の概念図

【図１６】　本発明の実施の形態８における情報処理装置の構成を示す概念図

【図１７】　本発明の実施の形態８におけるセキュア情報付き内蔵ＲＡＭ空間のスタック領域の状態図

【図１８】　本発明の実施の形態９における情報処理装置の構成を示す概念図

【図１９】　本発明の実施の形態９におけるセキュア情報付きＤＭＡの概念図

【図２０】　本発明の実施の形態１０における情報処理装置の構成を示す概念

図

【図２１】　本発明の実施の形態１０におけるセキュア情報付き演算部の概念図

【符号の説明】

１００　情報処理装置
１０１　ＣＰＵ
１０２　汎用レジスタファイル
１０３　汎用レジスタ
１０４　セキュア情報部
１０５　データ制御部
１０６　アドレス制御部
１０７　データ／アドレスバス
１０８　命令フェッチアドレス制御部
１０９　命令バッファ
１１０　ユーザメモリ空間（ＲＡＭ）
１１０ｐ　ユーザプログラム
１２０　セキュアメモリ空間（ＲＯＭ）
１２０ｐ　セキュアプログラム
２０１　セキュアメモリ空間
２０２　ユーザメモリ空間
２０３　データバス
２０４　アドレスバス
２０５　セキュア情報生成部
２０６　セキュア情報付き内蔵ＲＡＭ空間
２０７　セキュア情報付き内蔵ＲＡＭ空間内のセキュア情報部
２０８　ＣＰＵ
２０９　セキュア情報付き汎用レジスタ
２１０　セキュア情報付き汎用レジスタ内のセキュア情報部
２１１　データ出力制御部

２１２　外部空間

２１３　割り込み制御部

２１４　セキュア情報付き割り込み退避情報部

２１５　セキュア情報付き割り込み退避情報部内のセキュア情報部

２１６　セキュア情報付き命令デコーダ

２１７　セキュア情報付き命令デコーダ内のセキュア情報部

２１８　スタックポインタ

２１９　退避情報書き換え制御部

２２０　セキュア情報付きＤＭＡ

２２１　セキュア情報付きＤＭＡ内のセキュア情報部

２２２　セキュア情報付き演算部

２２３　セキュア情報付き演算部内のセキュア情報部

３００　第１の汎用レジスタ

３０１　第２の汎用レジスタ

３０２　第３の汎用レジスタ

３０３　第１のセキュア情報部

３０４　第２のセキュア情報部

３０５　第３のセキュア情報部

４００　状態レジスタ

５００　端末ＰＣ

５０１　ユーザＩＯ空間（ＲＡＭ）

５０２　セキュアＩＯ空間（ＲＡＭ）

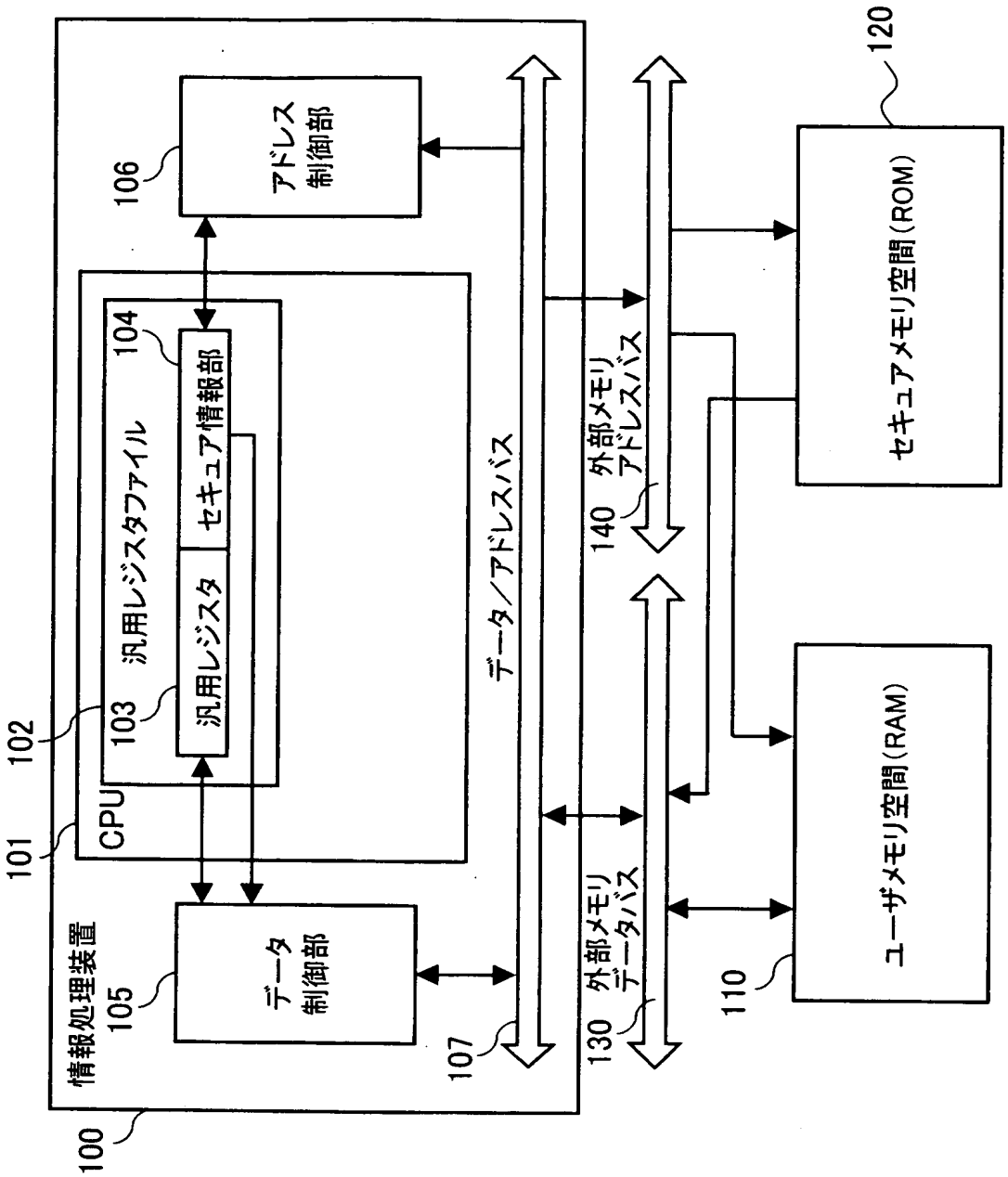
５０３　ＩＣカード

Ｓ５０３　デバッグ鍵

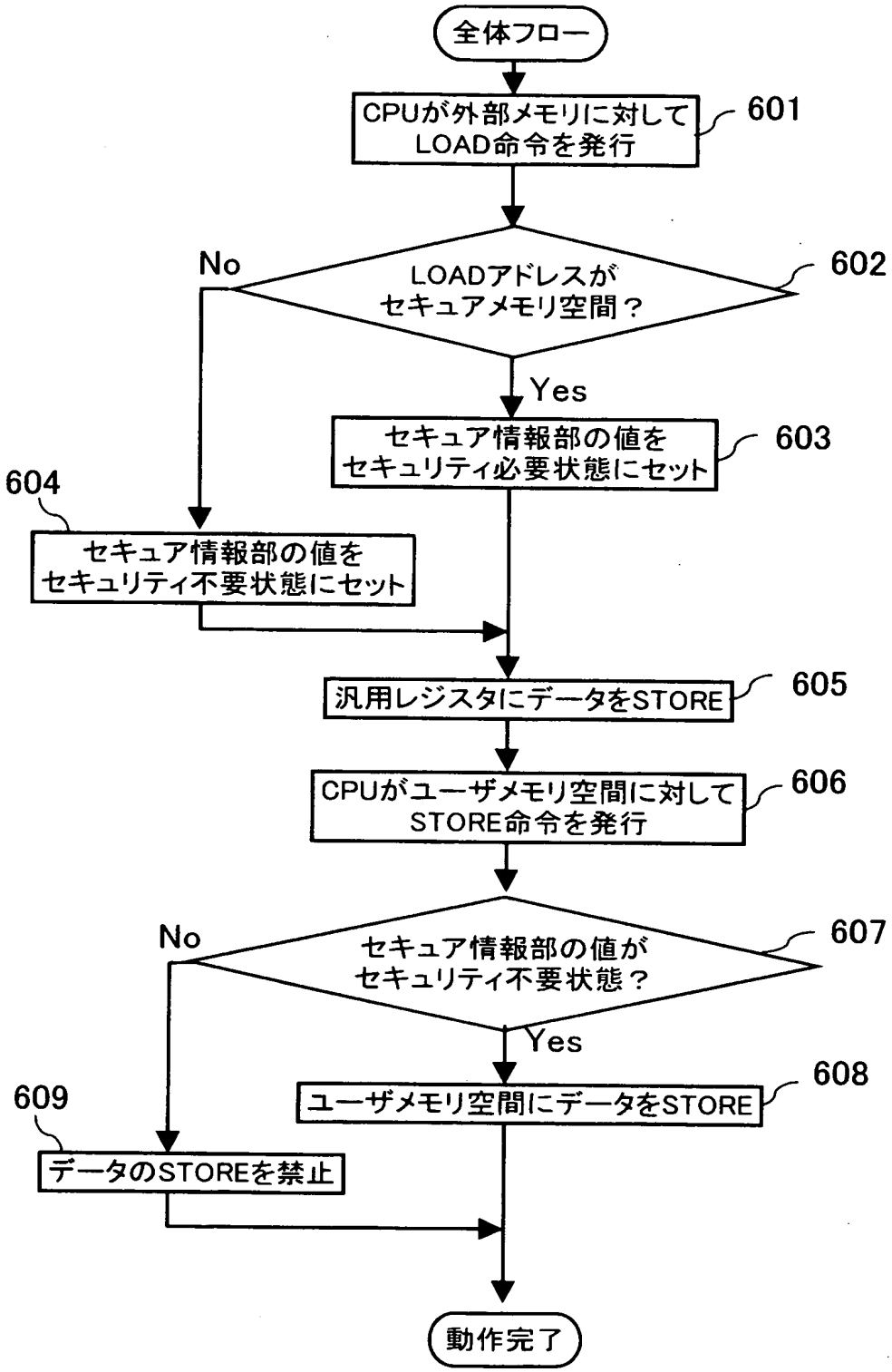
７０３ｃ　スタック退避情報

【書類名】　図面

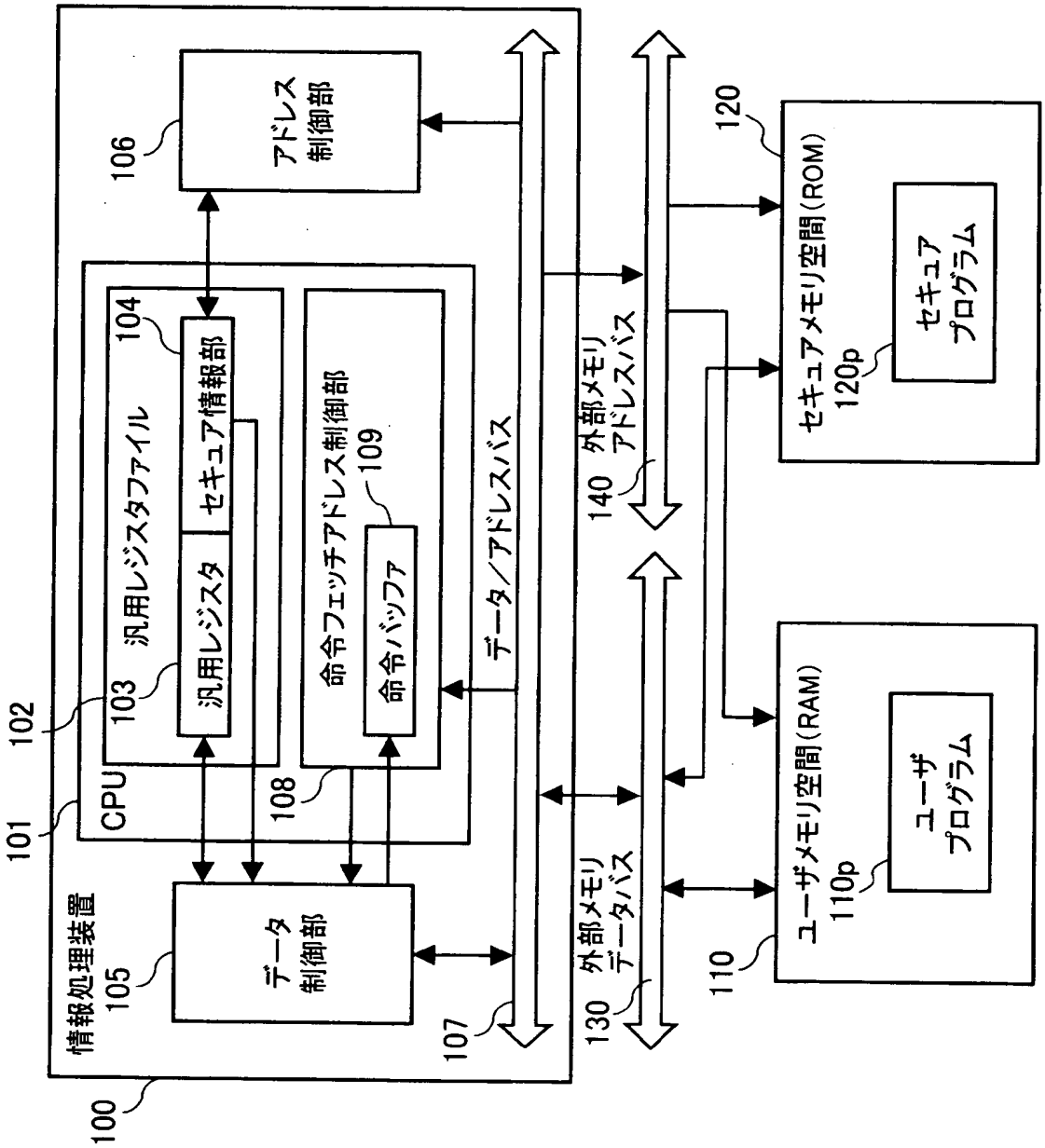
【図１】


情報処理装置
100
CPU
101
102
汎用レジスタ
103
セキュア情報部
104
汎用レジスタファイル
アドレス制御部
106
データ制御部
105
データ／アドレスバス
107
外部メモリアドレスバス
140
外部メモリデータバス
130
セキュアメモリ空間(ROM)
120
ユーザメモリ空間(RAM)
110

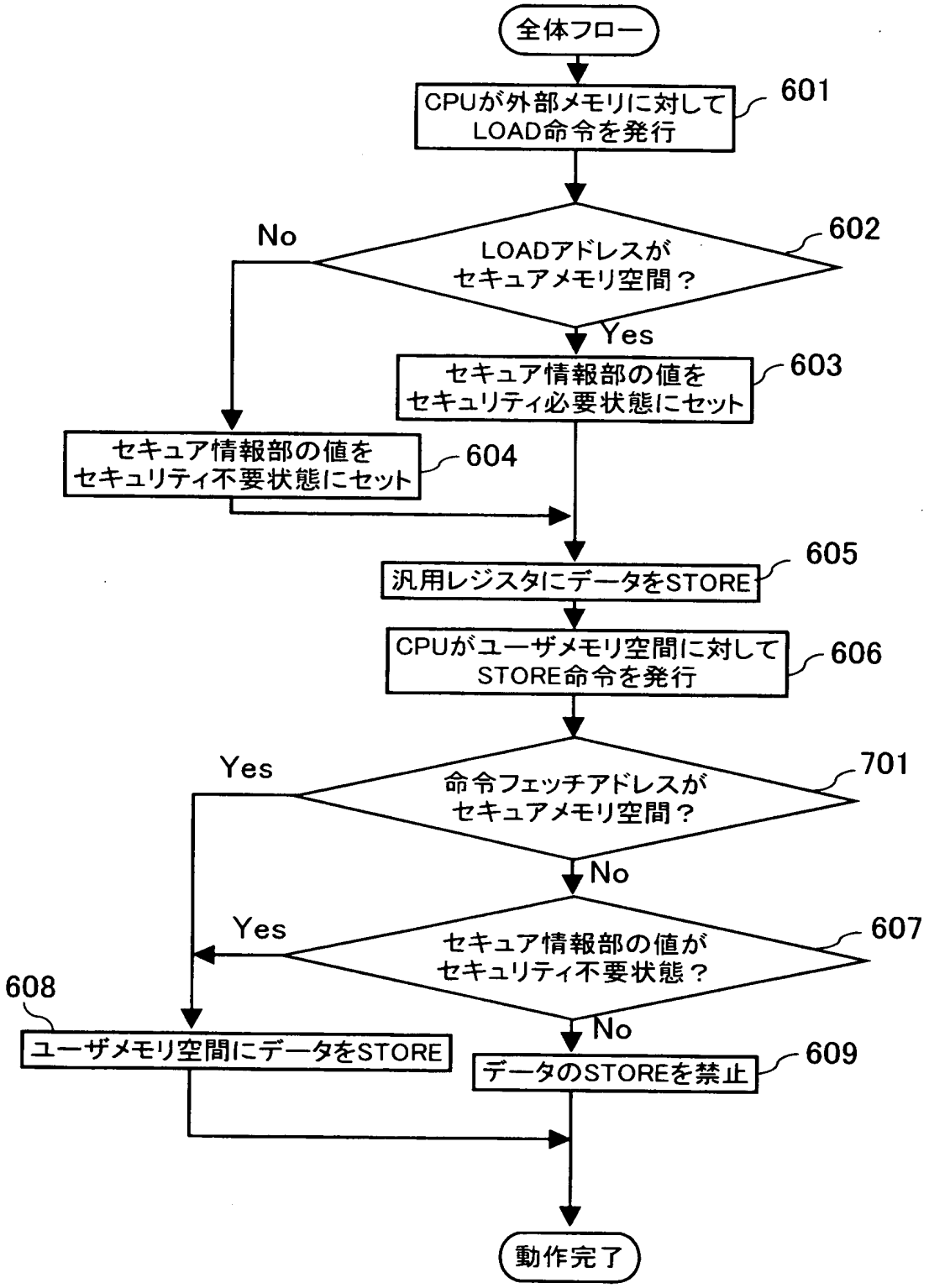
【図２】


全体フロー
CPUが外部メモリに対して
LOAD命令を発行
601
No
LOADアドレスが
セキュアメモリ空間？
602
Yes
セキュア情報部の値を
セキュリティ必要状態にセット
603
604
セキュア情報部の値を
セキュリティ不要状態にセット
汎用レジスタにデータをSTORE
605
CPUがユーザメモリ空間に対して
STORE命令を発行
606
No
セキュア情報部の値が
セキュリティ不要状態？
607
Yes
608
ユーザメモリ空間にデータをSTORE
609
データのSTOREを禁止
動作完了

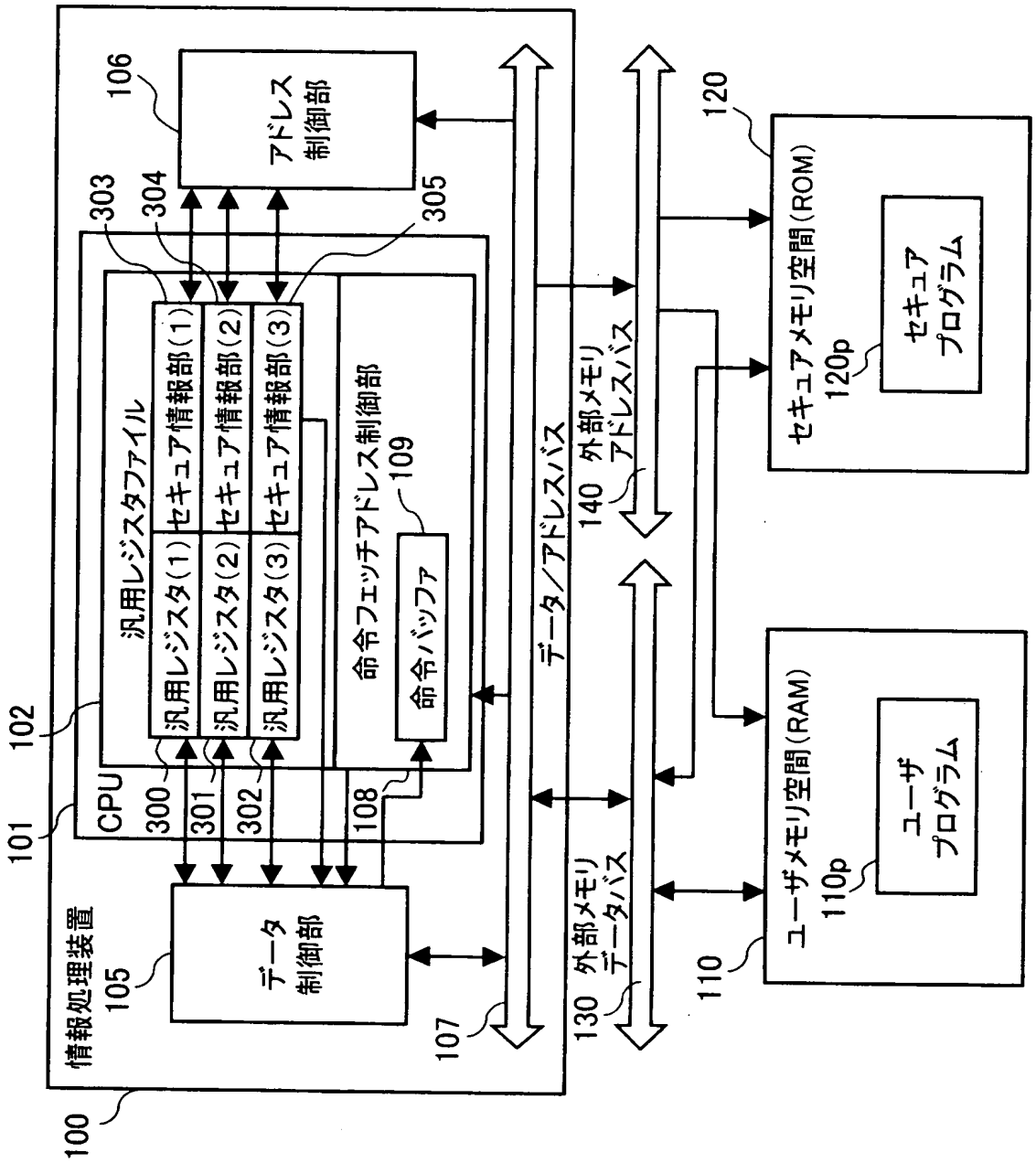
【図３】


情報処理装置
100
CPU
101
102
汎用レジスタファイル
103
汎用レジスタ
セキュア情報部
104
アドレス制御部
106
データ制御部
105
命令フェッチアドレス制御部
109
命令バッファ
108
データ／アドレスバス
107
外部メモリデータバス
130
外部メモリアドレスバス
140
セキュアメモリ空間(ROM)
120
120p
セキュアプログラム
ユーザメモリ空間(RAM)
110
110p
ユーザプログラム

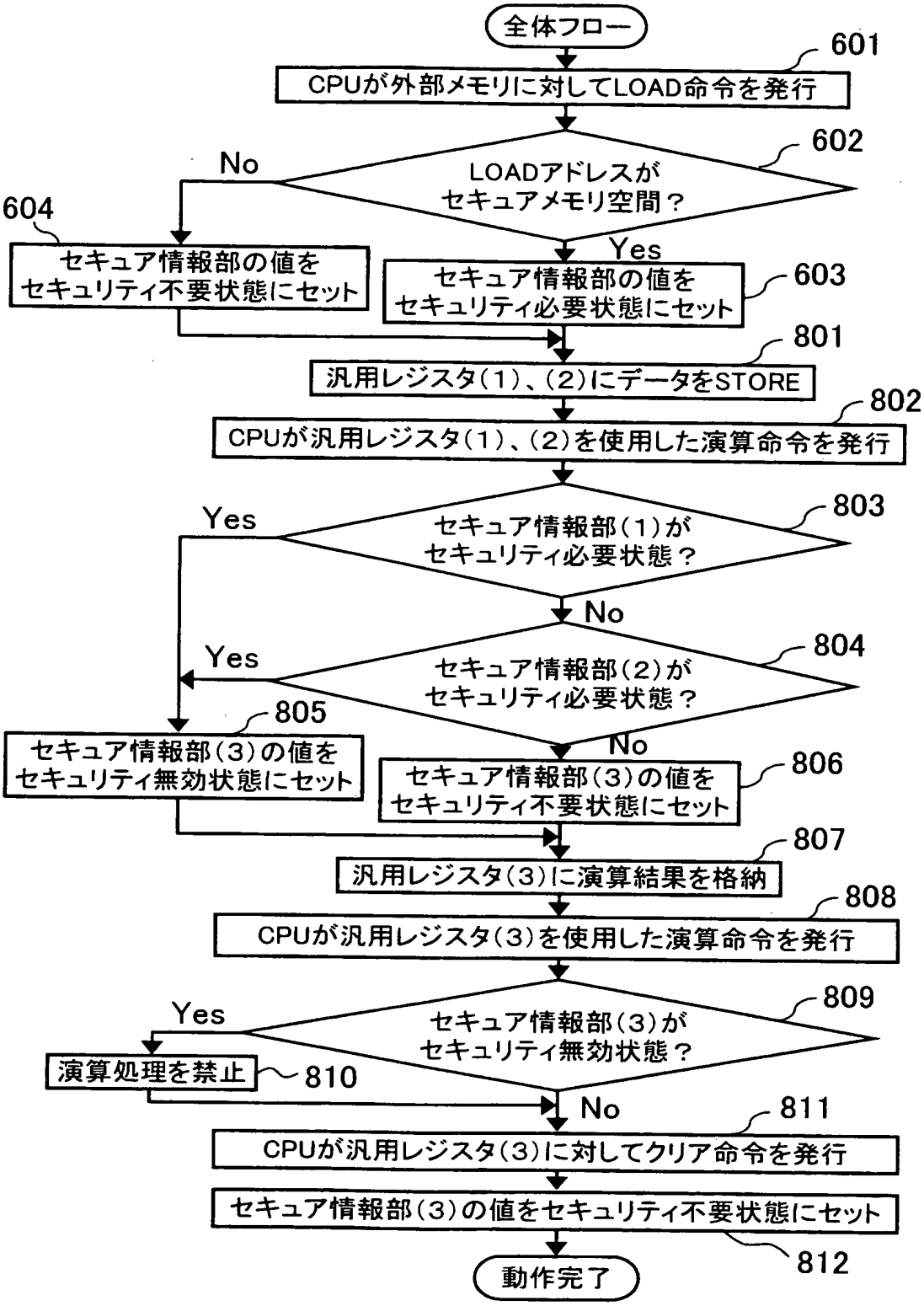
【図４】


全体フロー
CPUが外部メモリに対して
LOAD命令を発行
601
LOADアドレスが
セキュアメモリ空間？
602
No
Yes
セキュア情報部の値を
セキュリティ必要状態にセット
603
セキュア情報部の値を
セキュリティ不要状態にセット
604
汎用レジスタにデータをSTORE
605
CPUがユーザメモリ空間に対して
STORE命令を発行
606
命令フェッチアドレスが
セキュアメモリ空間？
701
Yes
No
セキュア情報部の値が
セキュリティ不要状態？
607
Yes
No
608
ユーザメモリ空間にデータをSTORE
データのSTOREを禁止
609
動作完了

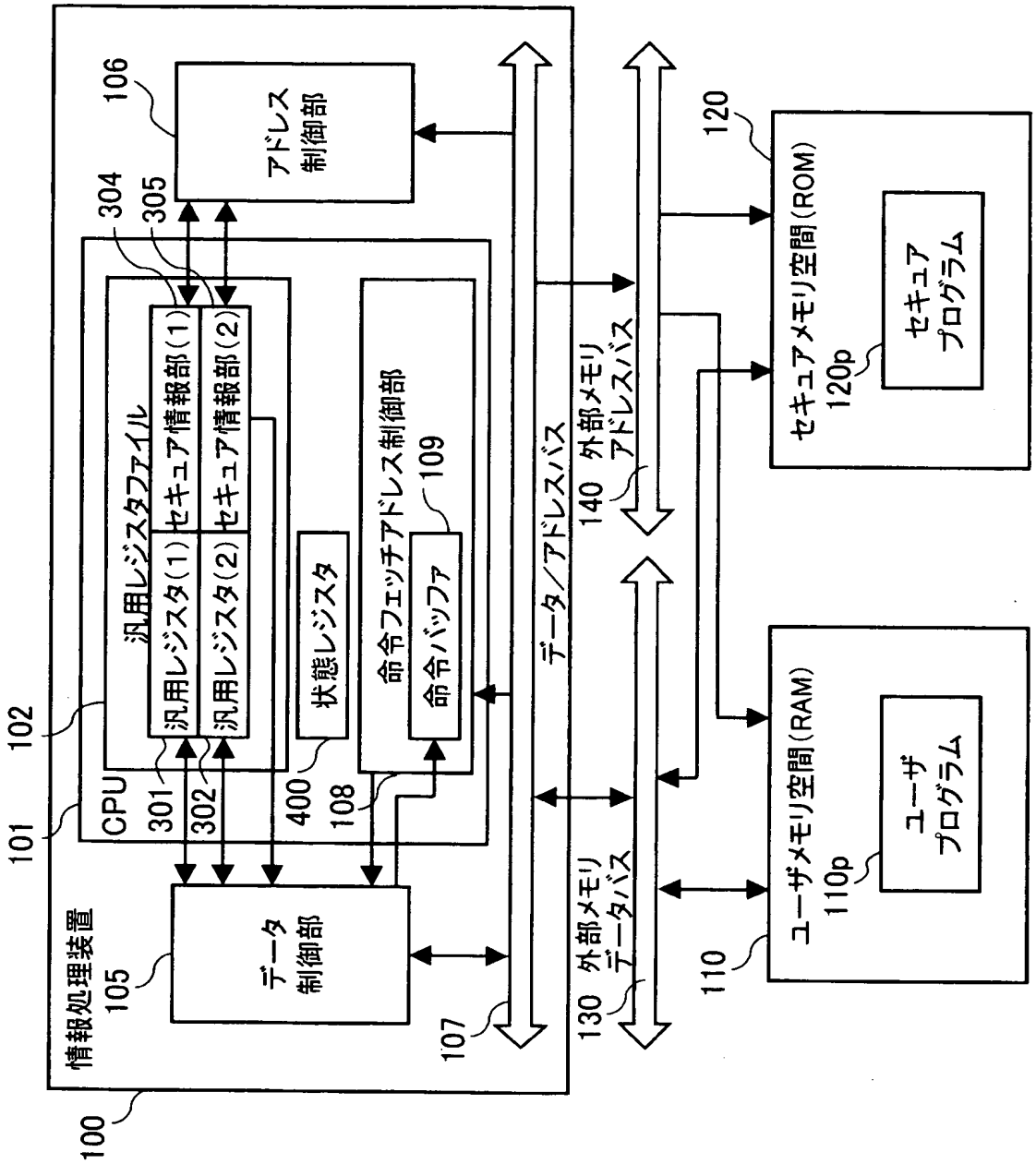
【図５】


情報処理装置
100
CPU
101
102
汎用レジスタファイル
汎用レジスタ(1)
汎用レジスタ(2)
汎用レジスタ(3)
セキュア情報部(1)
セキュア情報部(2)
セキュア情報部(3)
303
304
305
300
301
302
命令フェッチアドレス制御部
109
命令バッファ
108
アドレス制御部
106
データ制御部
105
107
データ／アドレスバス
外部メモリアドレスバス
140
外部メモリデータバス
130
セキュアメモリ空間(ROM)
120
120p
セキュアプログラム
ユーザメモリ空間(RAM)
110
110p
ユーザプログラム

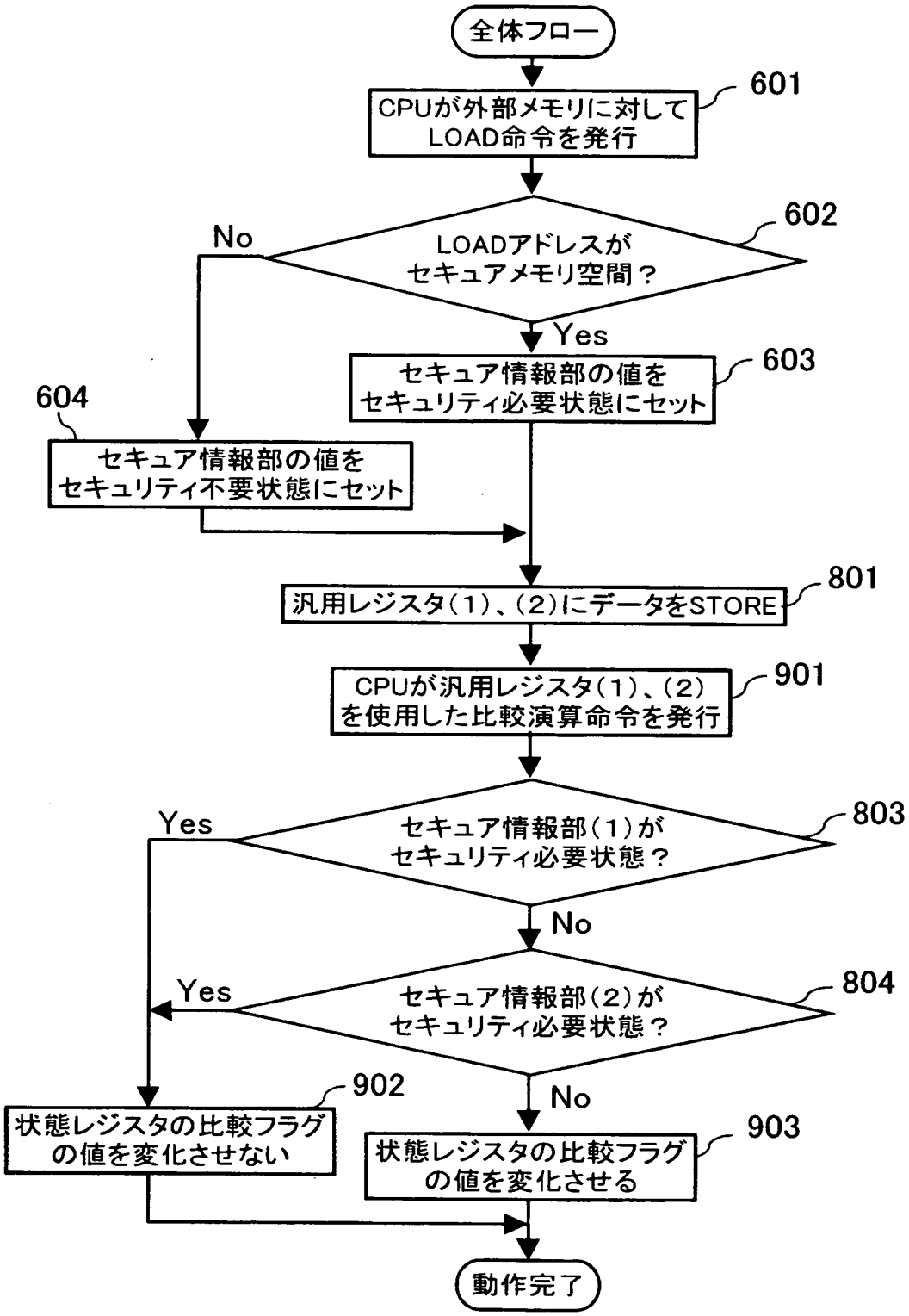
【図６】


全体フロー
601
CPUが外部メモリに対してLOAD命令を発行
602
LOADアドレスが
セキュアメモリ空間？
No
Yes
604
セキュア情報部の値を
セキュリティ不要状態にセット
セキュア情報部の値を
セキュリティ必要状態にセット
603
801
汎用レジスタ(1)、(2)にデータをSTORE
802
CPUが汎用レジスタ(1)、(2)を使用した演算命令を発行
803
セキュア情報部(1)が
セキュリティ必要状態？
Yes
No
804
セキュア情報部(2)が
セキュリティ必要状態？
Yes
No
805
セキュア情報部(3)の値を
セキュリティ無効状態にセット
セキュア情報部(3)の値を
セキュリティ不要状態にセット
806
807
汎用レジスタ(3)に演算結果を格納
808
CPUが汎用レジスタ(3)を使用した演算命令を発行
809
セキュア情報部(3)が
セキュリティ無効状態？
Yes
No
演算処理を禁止
810
811
CPUが汎用レジスタ(3)に対してクリア命令を発行
セキュア情報部(3)の値をセキュリティ不要状態にセット
812
動作完了

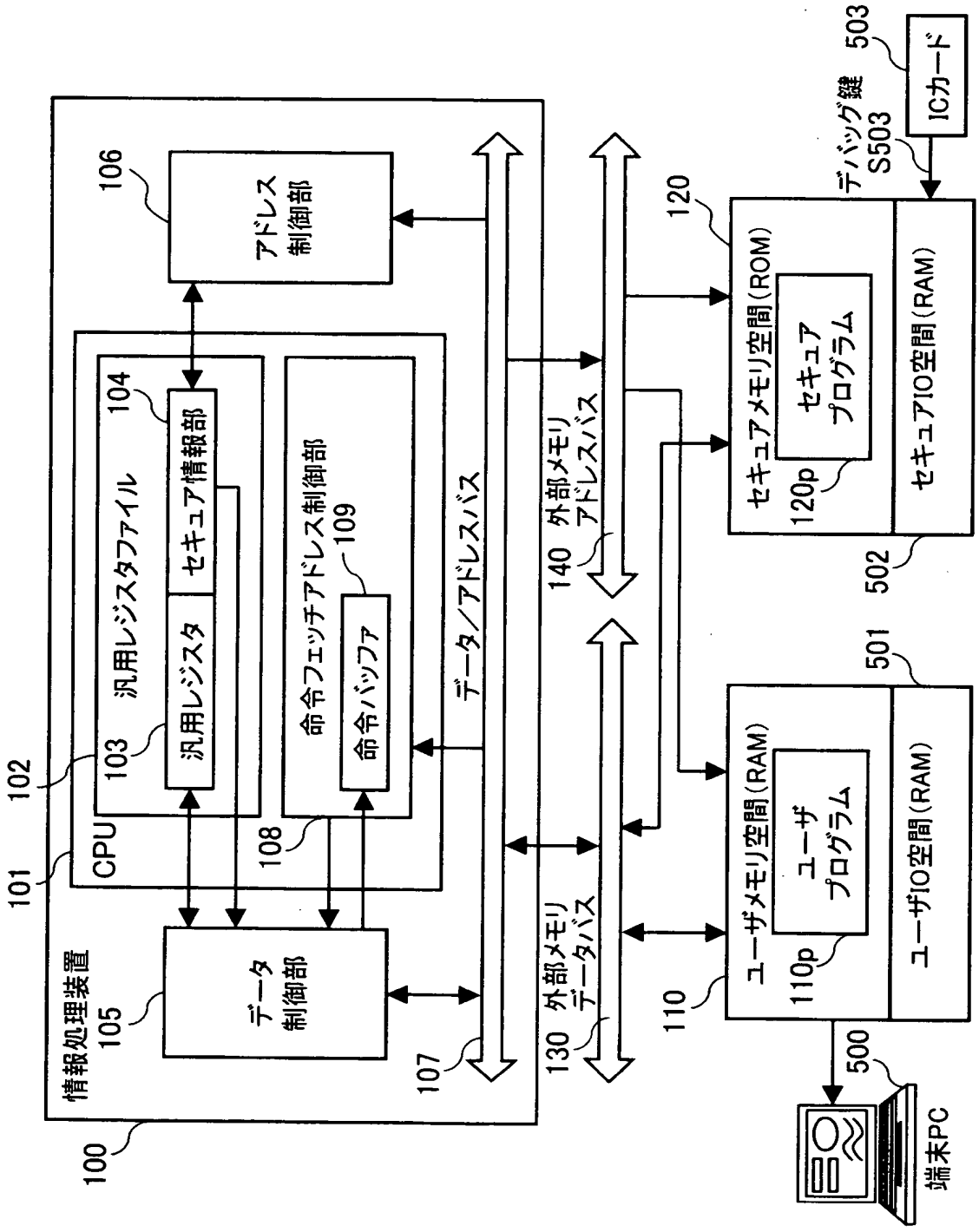
【図７】


情報処理装置
100
CPU
101
102
汎用レジスタファイル
汎用レジスタ(1)
汎用レジスタ(2)
セキュア情報部(1)
セキュア情報部(2)
301
302
304
305
状態レジスタ
400
命令フェッチアドレス制御部
109
命令バッファ
108
アドレス制御部
106
データ制御部
105
107
データ／アドレスバス
外部メモリデータバス
130
外部メモリアドレスバス
140
セキュアメモリ空間(ROM)
120
120p
セキュアプログラム
ユーザメモリ空間(RAM)
110
110p
ユーザプログラム

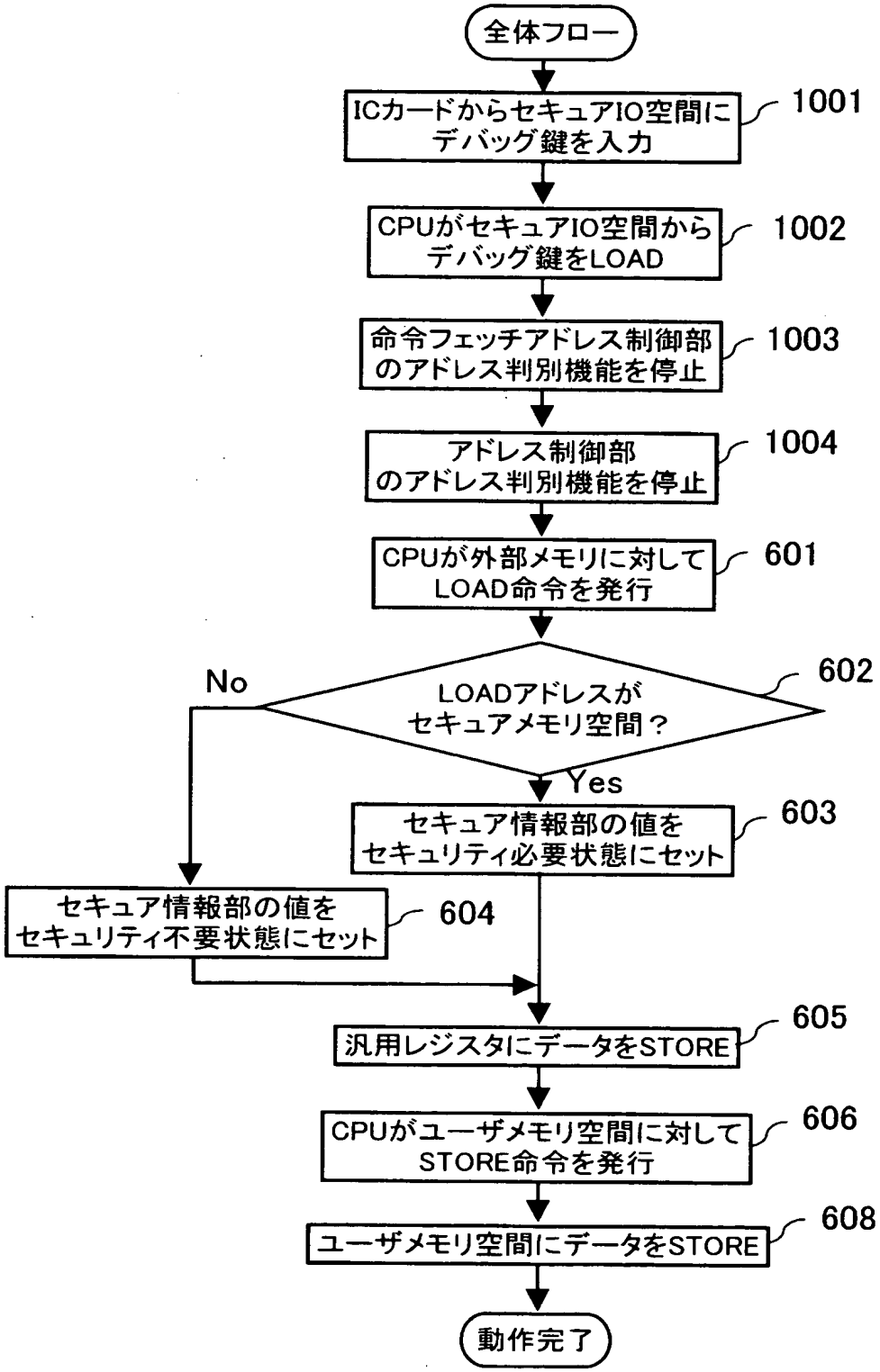
【図８】


全体フロー
CPUが外部メモリに対して
LOAD命令を発行
601
LOADアドレスが
セキュアメモリ空間？
602
No
Yes
セキュア情報部の値を
セキュリティ必要状態にセット
603
604
セキュア情報部の値を
セキュリティ不要状態にセット
汎用レジスタ(1)、(2)にデータをSTORE
801
CPUが汎用レジスタ(1)、(2)
を使用した比較演算命令を発行
901
セキュア情報部(1)が
セキュリティ必要状態？
803
Yes
No
セキュア情報部(2)が
セキュリティ必要状態？
804
Yes
No
902
状態レジスタの比較フラグ
の値を変化させない
903
状態レジスタの比較フラグ
の値を変化させる
動作完了

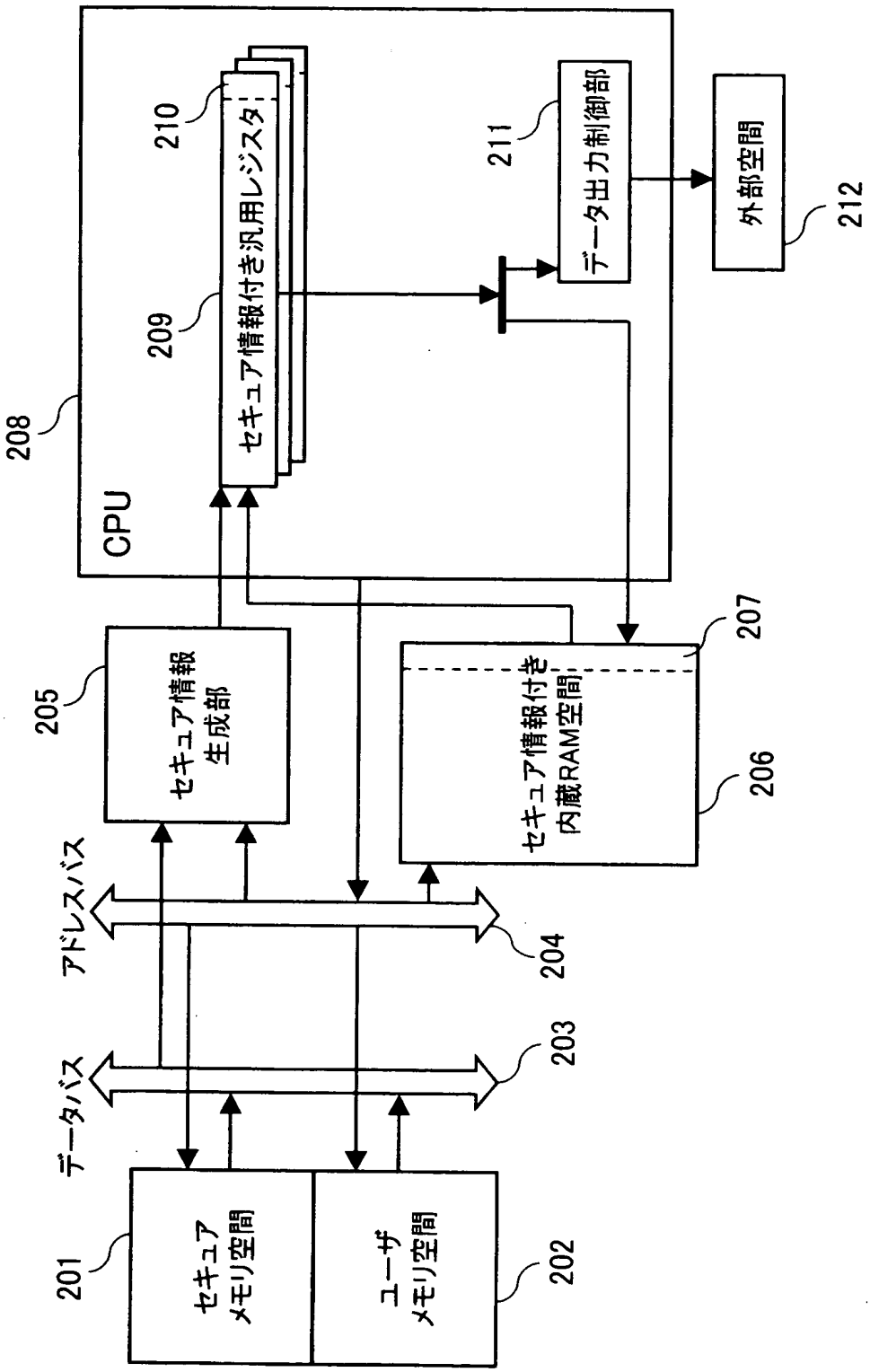
【図９】


情報処理装置
100
CPU
101
102
103
汎用レジスタファイル
104
汎用レジスタ
セキュア情報部
106
アドレス制御部
105
データ制御部
107
データ／アドレスバス
108
命令フェッチアドレス制御部
109
命令バッファ
130 外部メモリデータバス
140 外部メモリアドレスバス
110
ユーザメモリ空間(RAM)
110p
ユーザプログラム
501
ユーザIO空間(RAM)
120
セキュアメモリ空間(ROM)
120p
セキュアプログラム
502
セキュアIO空間(RAM)
デバッグ鍵 S503
503
ICカード
500
端末PC

【図１０】

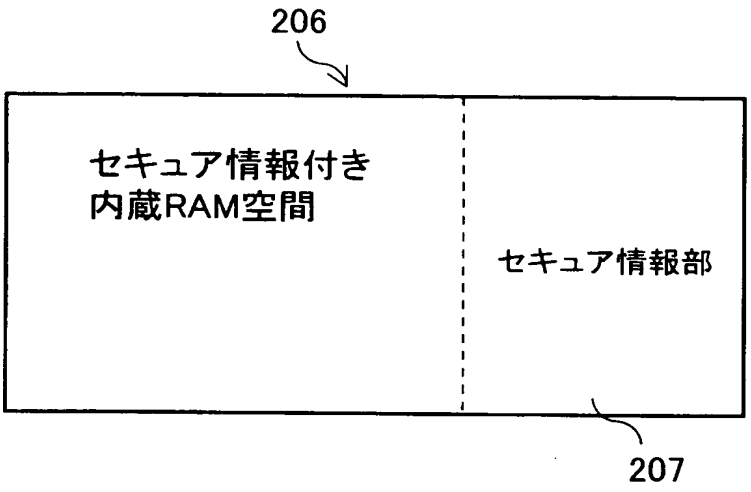

全体フロー
ICカードからセキュアIO空間にデバッグ鍵を入力
1001
CPUがセキュアIO空間からデバッグ鍵をLOAD
1002
命令フェッチアドレス制御部のアドレス判別機能を停止
1003
アドレス制御部のアドレス判別機能を停止
1004
CPUが外部メモリに対してLOAD命令を発行
601
LOADアドレスがセキュアメモリ空間？
602
No
Yes
セキュア情報部の値をセキュリティ必要状態にセット
603
セキュア情報部の値をセキュリティ不要状態にセット
604
汎用レジスタにデータをSTORE
605
CPUがユーザメモリ空間に対してSTORE命令を発行
606
ユーザメモリ空間にデータをSTORE
608
動作完了

【図１１】

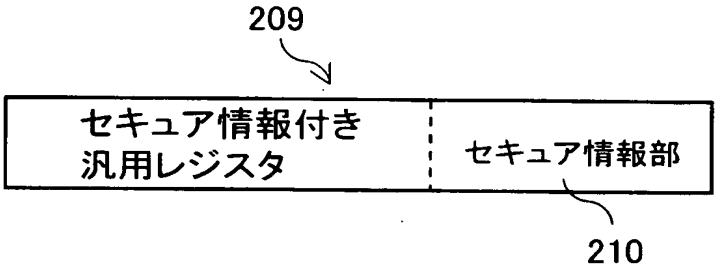

CPU
208
セキュア情報付き汎用レジスタ
209
210
データ出力制御部
211
外部空間
212
セキュア情報
生成部
205
セキュア情報付き
内蔵RAM空間
207
206
アドレスバス
204
データバス
203
セキュア
メモリ空間
201
ユーザ
メモリ空間
202

【図１２】

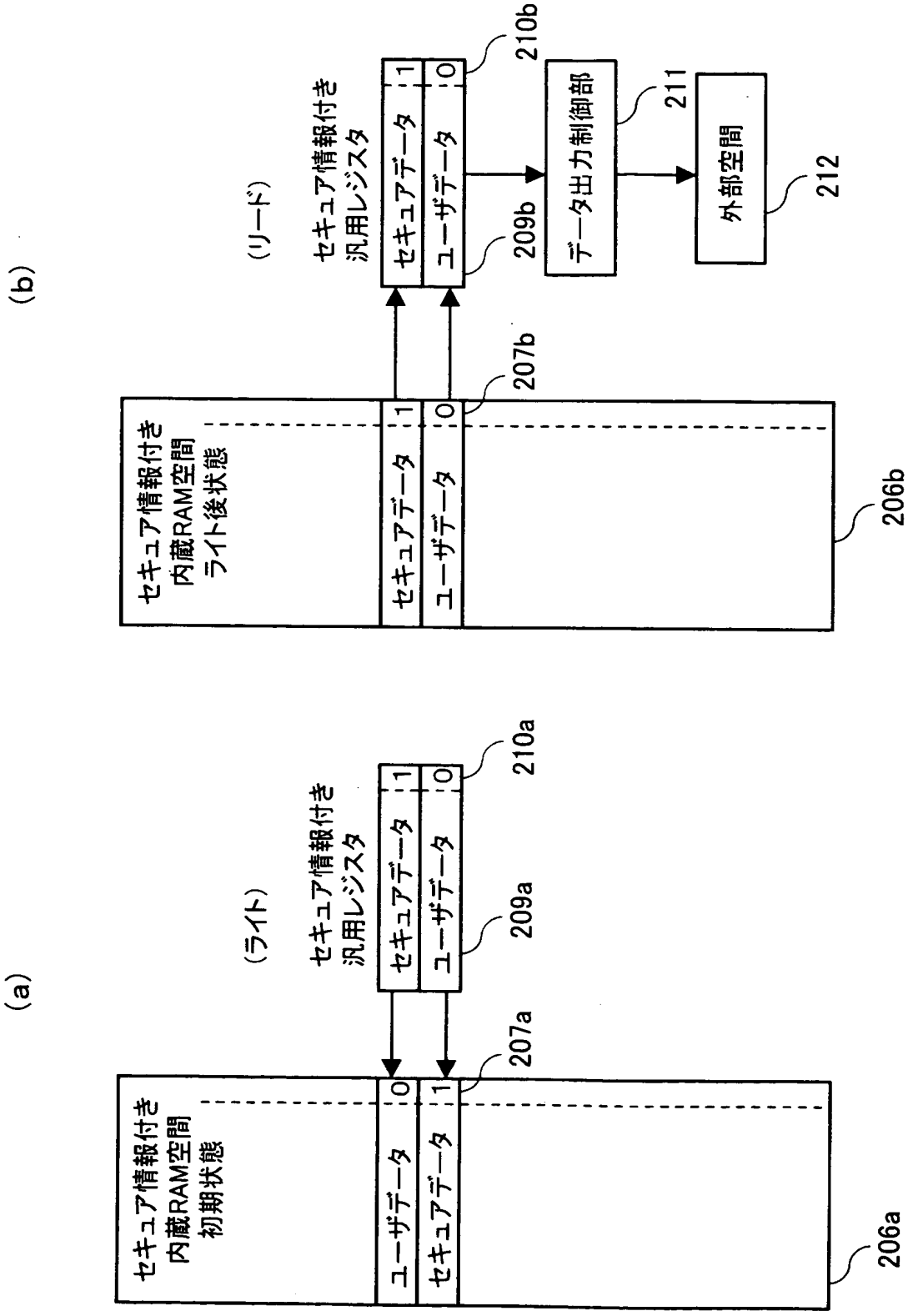
(a)


206
セキュア情報付き
内蔵RAM空間
セキュア情報部
207

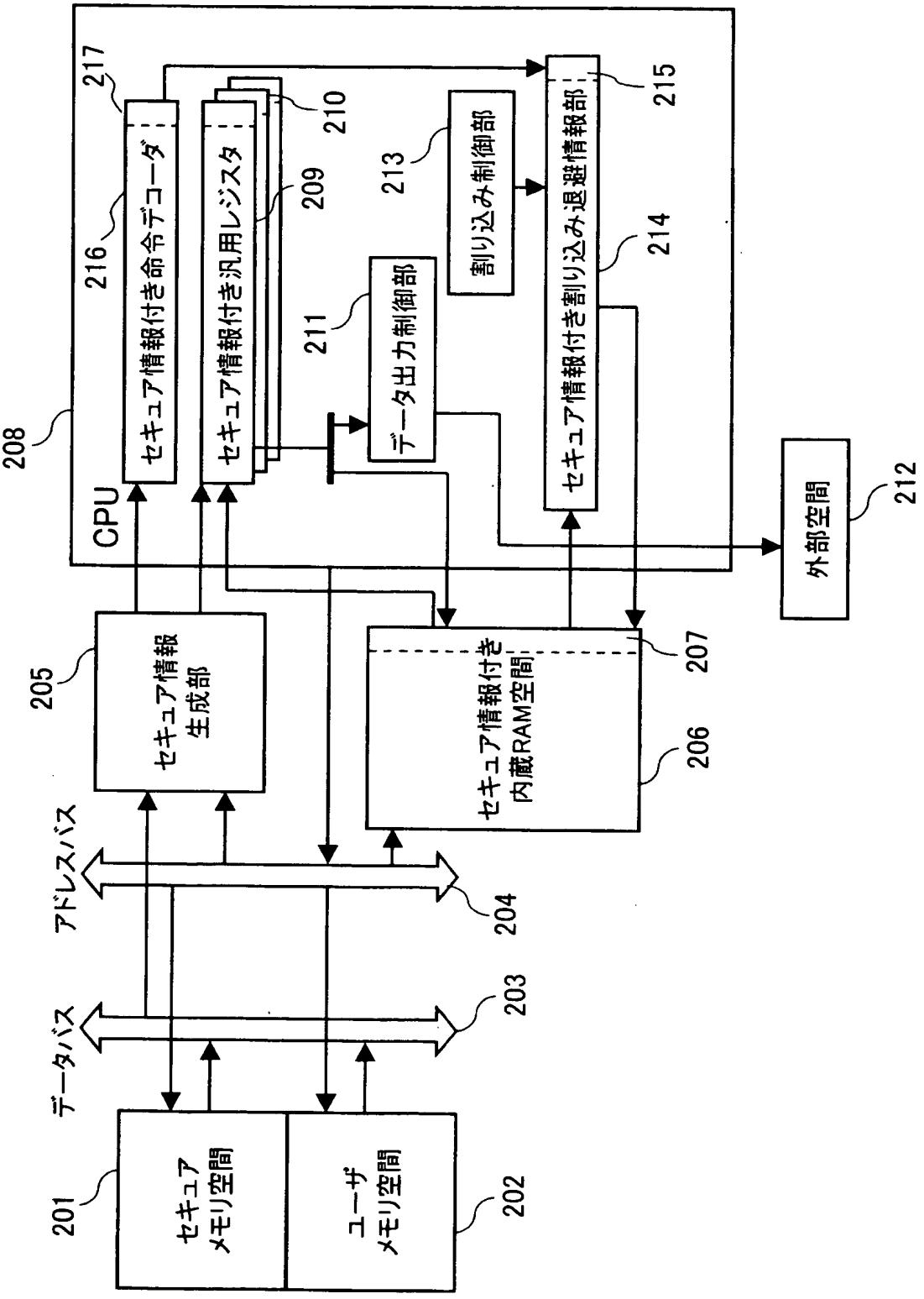
(b)


209
セキュア情報付き
汎用レジスタ
セキュア情報部
210

【図１３】

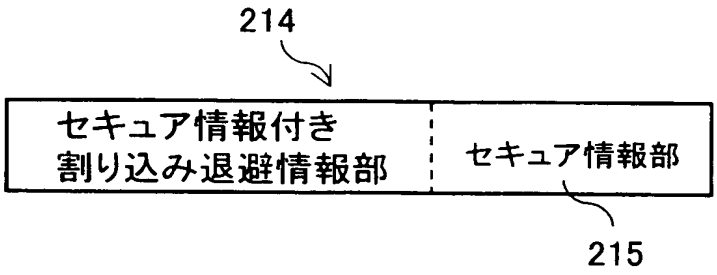

(a)
セキュア情報付き
内蔵RAM空間
初期状態
ユーザデータ
セキュアデータ
0
1
206a
207a
(ライト)
セキュア情報付き
汎用レジスタ
ユーザデータ
セキュアデータ
209a
210a
(b)
セキュア情報付き
内蔵RAM空間
ライト後状態
ユーザデータ
セキュアデータ
206b
207b
(リード)
セキュア情報付き
汎用レジスタ
ユーザデータ
セキュアデータ
209b
210b
データ出力制御部
211
外部空間
212

【図１４】

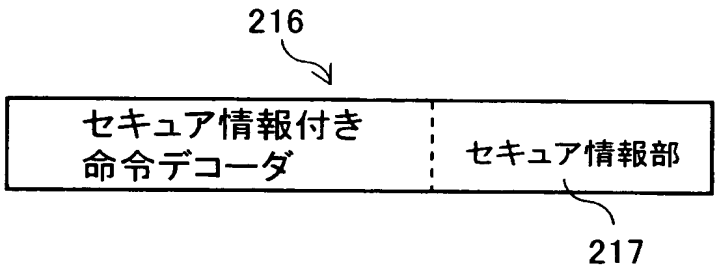

CPU
208
セキュア情報付き命令デコーダ
216
217
セキュア情報付き汎用レジスタ
209
210
データ出力制御部
211
割り込み制御部
213
セキュア情報付き割り込み退避情報部
214
215
外部空間
212
セキュア情報
生成部
205
セキュア情報付き
内蔵RAM空間
206
207
アドレスバス
204
データバス
203
セキュア
メモリ空間
201
ユーザ
メモリ空間
202

【図１５】

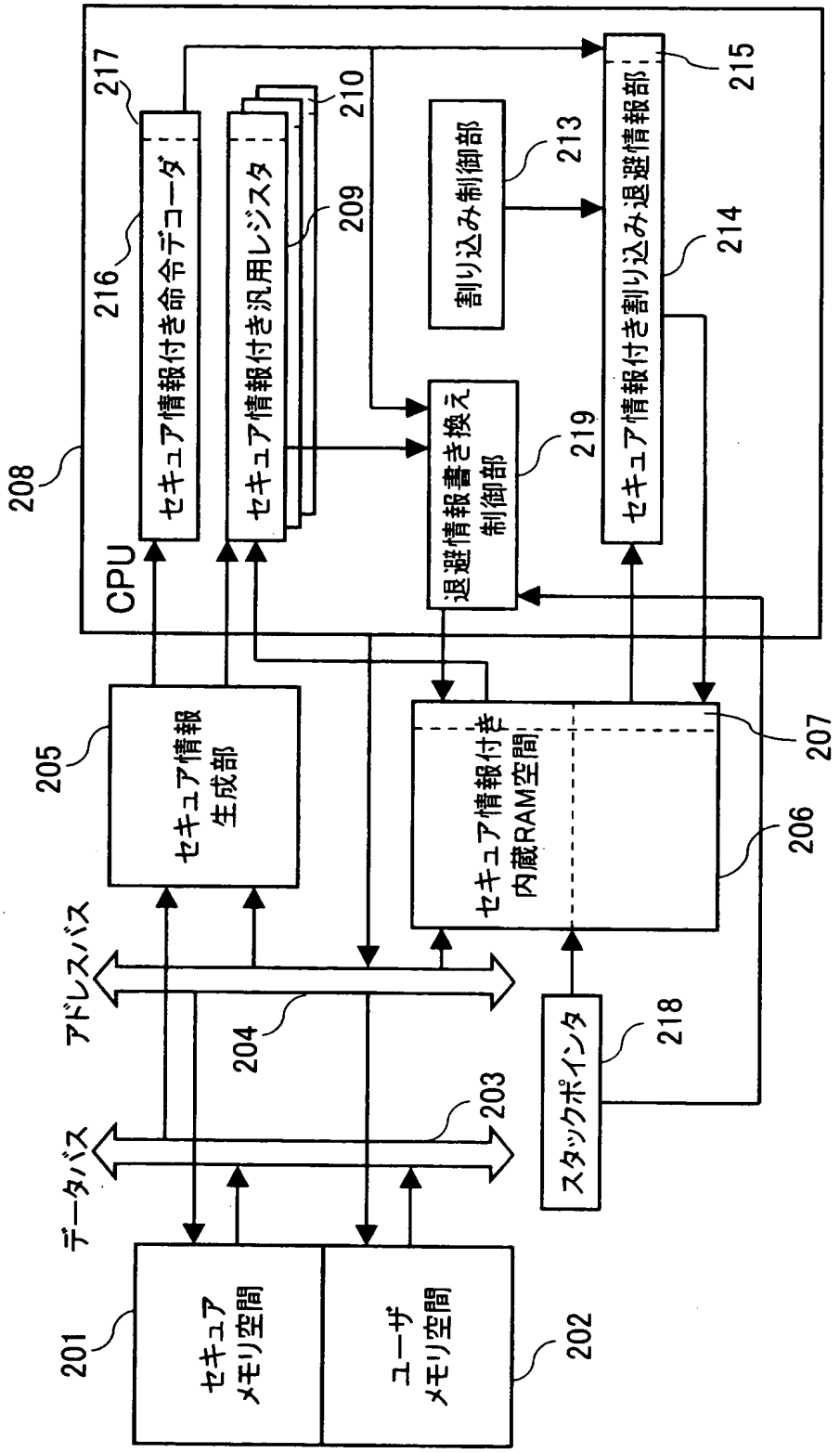
(a)


214
セキュア情報付き
割り込み退避情報部
セキュア情報部
215

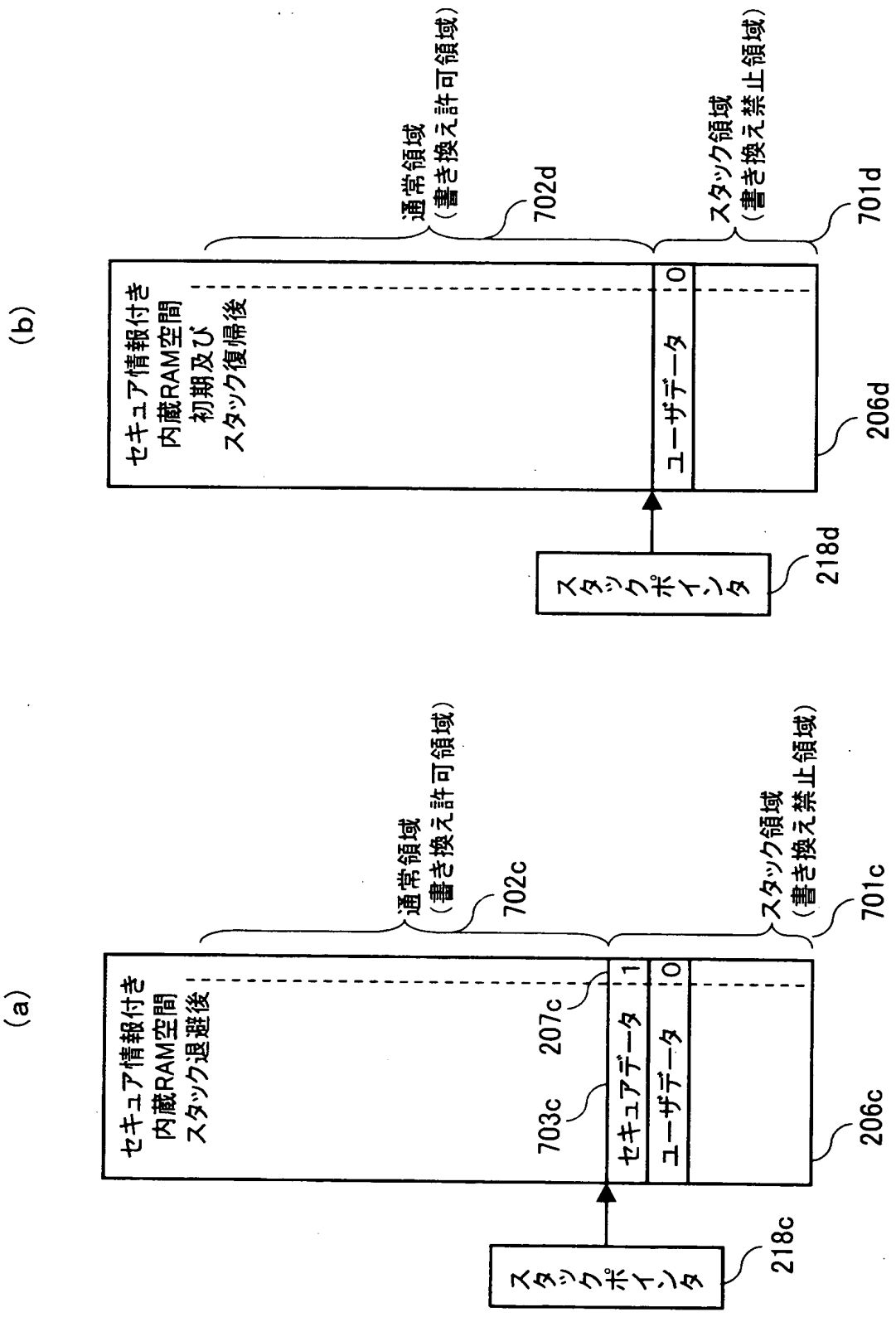
(b)


216
セキュア情報付き
命令デコーダ
セキュア情報部
217

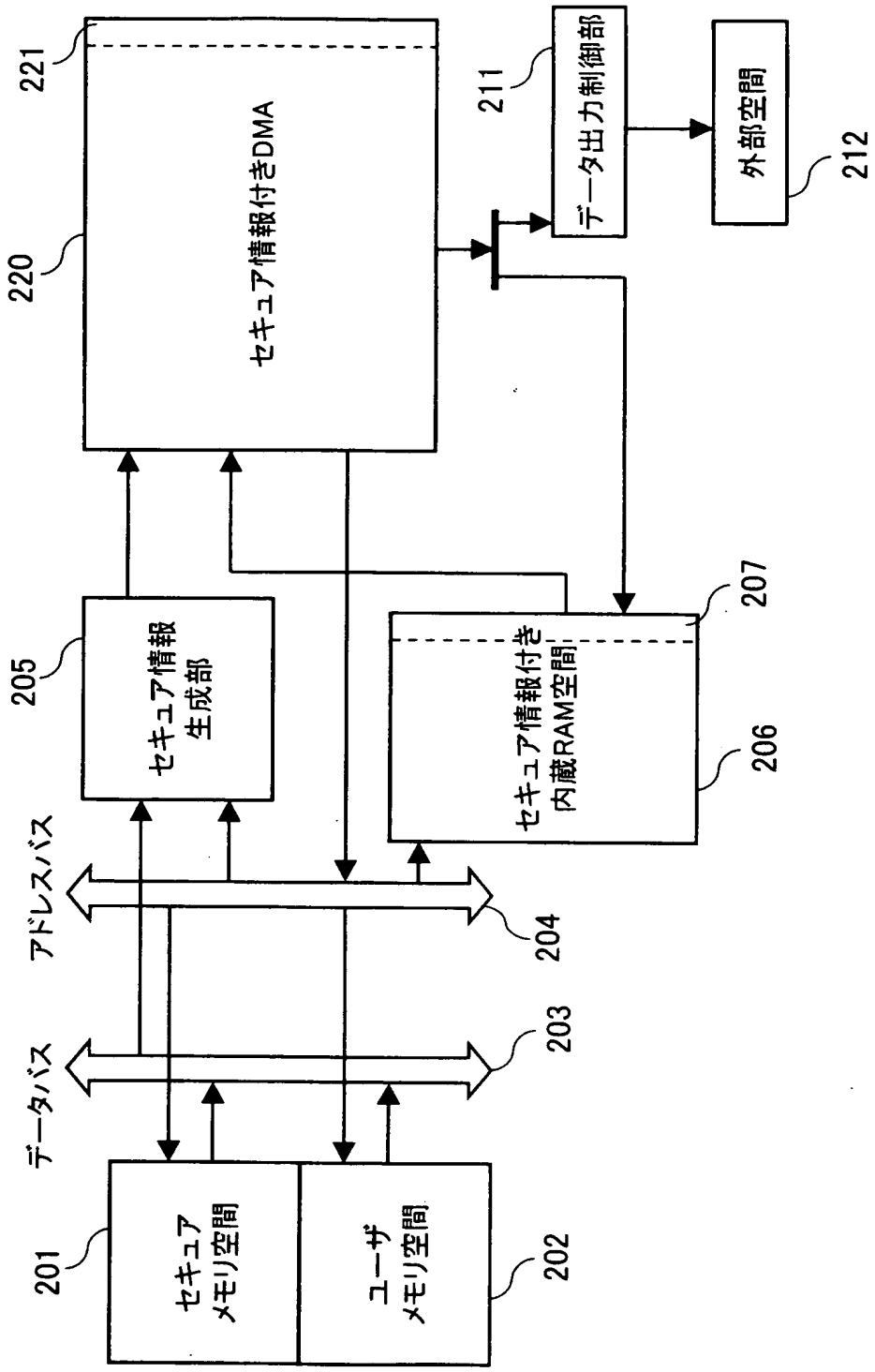
【図１６】


CPU
208
セキュア情報付き命令デコーダ
216
217
セキュア情報付き汎用レジスタ
209
210
割り込み制御部
213
セキュア情報付き割り込み退避情報部
214
215
退避情報書き換え制御部
219
セキュア情報生成部
205
セキュア情報付き内蔵RAM空間
207
206
アドレスバス
204
データバス
203
スタックポインタ
218
セキュアメモリ空間
201
ユーザメモリ空間
202

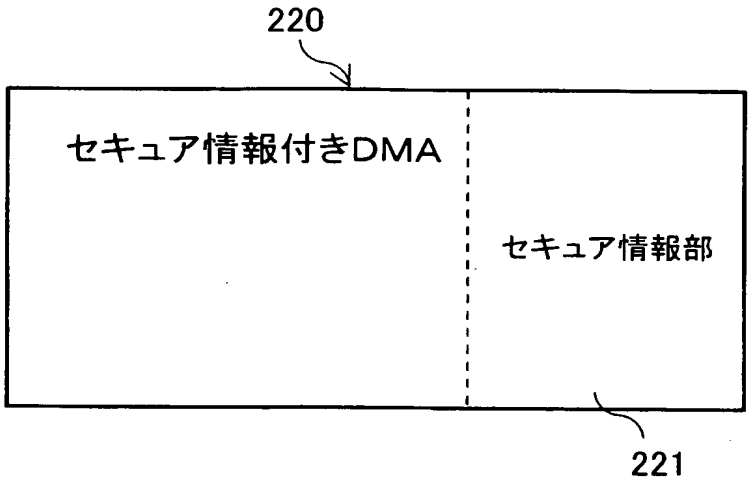
【図１７】


(a)
セキュア情報付き
内蔵RAM空間
スタック退避後
通常領域
（書き換え許可領域）
702c
スタック領域
（書き換え禁止領域）
701c
207c
703c
1
0
セキュアデータ
ユーザデータ
206c
スタック
ポインタ
218c
(b)
セキュア情報付き
内蔵RAM空間
初期及び
スタック復帰後
通常領域
（書き換え許可領域）
702d
スタック領域
（書き換え禁止領域）
701d
0
ユーザデータ
206d
スタック
ポインタ
218d

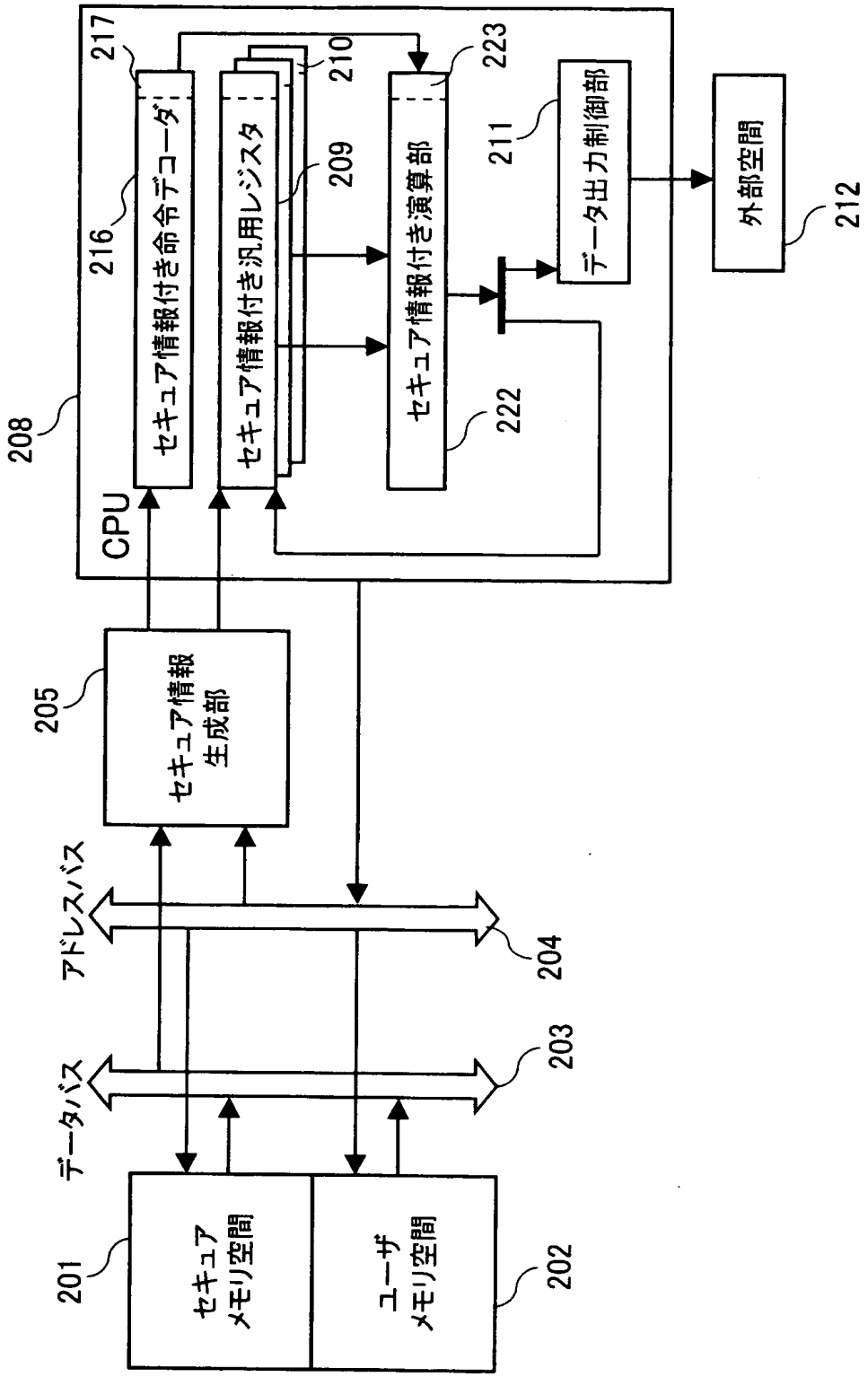
【図１８】


221
220
セキュア情報付きDMA
211
データ出力制御部
外部空間
212
205
セキュア情報
生成部
207
セキュア情報付き
内蔵RAM空間
206
アドレスバス
204
データバス
203
201
セキュア
メモリ空間
ユーザ
メモリ空間
202

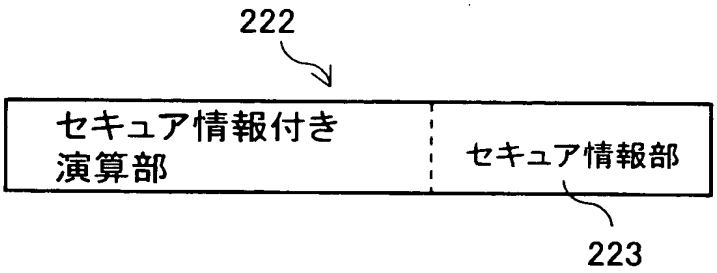
【図１９】



【図２０】


CPU
208
セキュア情報付き命令デコーダ
216
217
セキュア情報付き汎用レジスタ
209
210
セキュア情報付き演算部
222
223
データ出力制御部
211
外部空間
212
セキュア情報
生成部
205
アドレスバス
204
データバス
203
セキュア
メモリ空間
201
ユーザ
メモリ空間
202

【図２１】



【書類名】　要約書

【要約】

【課題】　従来の特権モードによるメモリ保護ではなく、セキュアメモリ空間のデータや命令を外部に読み出すことをできなくし、従来技術で行われる悪用を回避する。

【解決手段】　ユーザメモリ空間１１０から汎用レジスタ１０３にデータを転送した場合はセキュア情報部１０４の値をセキュリティ不要状態とし、セキュアメモリ空間１２０から汎用レジスタ１０３にデータを転送した場合はセキュア情報部１０４の値をセキュリティ必要状態とし、セキュア情報部１０４の値がセキュリティ必要状態である汎用レジスタ１０３からユーザメモリ空間１１０へのデータ転送が禁止されるようにする制御を行うことによって、セキュアメモリ空間１２０上の暗号鍵が読まれることを防ぐ。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０２６８１０
受付番号	５０３００１７４５０８
書類名	特許願
担当官	第二担当上席　　００９１
作成日	平成１５年　２月１４日

＜認定情報・付加情報＞

【提出日】　平成15年 2月 4日

次頁無

出証特２００３－３０８９５８７

特願２００３－０２６８１０

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社